U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 475.1

Approved: 12-10-04
Review: 12-10-06
Expires: 12-10-08

SUBJECT: COUNTERINTELLIGENCE PROGRAM

1. OBJECTIVES. To establish Counterintelligence (CI) Program requirements and responsibilities for the Department of Energy (DOE), including the National Nuclear Security Administration (NNSA). Pursuant to Executive Order (E.O.) 12333 and *DOE Procedures for Intelligence Activities* (October 1992), the Department will—

   a. conduct CI activities to protect DOE information (e.g. classified, unclassified controlled information, proprietary, unclassified, and economic information affecting national security), personnel, and assets from international terrorist activities and from intelligence collection by or on behalf of foreign powers or entities;

   b. detect and deter insiders who engage in activities on behalf of a foreign intelligence service or international terrorist entity; and

   c. provide graded levels of CI Program activity and support for DOE programs in accordance with the potential risks.

2. CANCELLATION. DOE 5670.3, *Counterintelligence Program,* dated 9-4-92. Cancellation of an Order does not, by itself, modify or otherwise affect any contractual obligation to comply with the Order. Canceled Orders that are incorporated by reference in a contract remain in effect until the contract is modified to delete the references to the requirements in the canceled Orders.

3. APPLICABILITY.

   a. Primary DOE Organizations, Including National Nuclear Security Administration (NNSA) Organizations. Except for the exclusions in paragraph 3c, this Order applies to all Primary DOE Organizations and the DOE administered Power Marketing Administrations (see Attachment 1 for a complete list of Primary DOE Organizations). This Order automatically applies to Primary DOE Organizations created after it is issued.

      The NNSA Administrator will ensure that NNSA employees and contractors comply with their respective responsibilities under this Order.

   b. Site/Facility Management Contractors.

      (1) Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Order that will apply to site/facility management contractors whose contracts include the CRD.

(2) The CRD must be included in all site/facility management contracts for contractors that are required to conduct CI Programs.

(3) This Order does not apply to other than site/facility management contractors. Any application of requirements of this Order to other than site/facility management contractors will be communicated separately.

(4) Secretarial officers are responsible for telling contracting officers which site/facility management contracts are affected by this Order. Once notified, the contracting officer is responsible for incorporating the CRD into the laws, regulations, and DOE directives clause of each affected site/facility management contract.

(5) As the laws, regulations, and DOE directives clause of a site/facility management contract states, regardless of the performer of the work, the site/facility management contractor is responsible for compliance with the requirements of the CRD.

(a) Affected site/facility management contractors are responsible for notifying subcontractors at any tier of the requirements of the CRD to the extent necessary to ensure the site/facility management contractor's compliance with the applicable requirements.

(b) In doing so, the contractor will not impose unnecessary or imprudent requirements to subcontractors. That is, the contractor will—

1 ensure that it and its subcontractors comply with the requirements of the CRD and

2 only incur costs that would be incurred by a prudent person in the conduct of competitive business.

c. Exclusions. None.

4. REQUIREMENTS.

a. Background. Pursuant to E.O. 12333 and *DOE Procedures for Intelligence Activities*, it is DOE policy to protect programs, resources, facilities, and personnel from intelligence collection by or on behalf of international terrorists or foreign powers or entities and related threats through implementation of an effective, efficient CI program. Since the signing of Presidential Decision Directive (PDD) 61, *U.S. Department of Energy Counterintelligence Program (U)* (February 1998), the Department has taken aggressive measures to strengthen the CI program now administered by the DOE Office of Counterintelligence

(OCI) and the NNSA Office of Defense Nuclear Counterintelligence (ODNCI). This Order reflects the current CI program scope and requirements.

b. Program Organization.

(1) The CI Program is comprised of the DOE OCI and the NNSA ODNCI.

(2) The OCI includes the following programs:

(a) Analysis;

(b) Operations and Investigations;

(c) Plans, Policy, Training and Awareness;

(d) Information and Special Technologies;

(e) Inspections; and

(f) CI Evaluation Program (CIEP), which includes the Polygraph Program.

(3) These programs are shared resources between OCI and ODNCI. Both the OCI Director and the ODNCI Chief direct the managers of these programs, with the exception of the Inspections and Polygraph programs, which are directed solely by the OCI Director.

(4) The OCI Director is responsible for administrative management of the OCI program directors, their staffs and related support staffs, and OCI Headquarters activities. The OCI Director executes these responsibilities in coordination with the ODNCI Chief.

(5) The CI Program also consists of specific field elements that perform CI functions. The OCI Director and ODNCI Chief manage these field elements in accordance with this Order. To maintain a centrally managed CI Program and achieve a graded approach to CI across DOE [see paragraph 4(e), below], local CI offices have been established at specific DOE locations. Some of these offices act as servicing CI offices for additional facilities because of existing organizational relationships or geographic proximity. This Order does not limit the authority of the OCI Director and ODNCI Chief to add or eliminate programs or change the Headquarters or field organizational structure to execute the CI Program effectively.

(6) A close, cooperative relationship between OCI and ODNCI management is essential to the successful execution of the DOE CI mission.

c. Program Independence.

(1) To ensure that the program operates independent of other DOE organizations, the OCI Director will report directly to the Secretary and the ODNCI Chief will report directly to the NNSA Administrator. Both also will have direct access to all Departmental officials and contractors. The ODNCI Chief also will have direct access to the Secretary.

(2) All DOE elements will cooperate fully with OCI/ODNCI program activities and will make available all appropriate files/records (regardless of media), facilities, activities, security information, information technology (IT) systems, and databases that are within their purview following verification of access authorization and need-to-know.

d. Program Implementation. To support DOE response to threats posed by foreign powers or entities and international terrorists attempting to collect intelligence information, the CI Program Headquarters and field elements will conduct the following activities.

(1) Analyze and assess the threat posed by these entities and their activities and advise the Department/Administration on potential threats.

(2) Develop and execute a comprehensive CI awareness program that includes regular briefings to ensure that personnel are aware of their responsibilities in support of the CI Program. Briefings will be integrated into or provided in conjunction with required security briefings (e.g., new hires' initial briefings and comprehensive and annual refresher briefings).

(3) An effective CI awareness program for employees includes the following.

(a) Initial and comprehensive briefings on CI. Topics include but are not limited to overview of the foreign intelligence collection and international terrorist threat, espionage indicators, and reporting requirements.

(b) Annual refresher briefings designed to reinforce and update awareness of CI issues and employees' responsibilities.

(c) Additional awareness briefings and training for specific employee groups as identified in site-specific awareness plans.

NOTE: Portions of the awareness program may be coordinated with the security awareness program at the discretion of local site officials.

(4) Conduct investigations and inquiries on incidents of CI/counterterrorism concern.

(5) Develop and conduct IT-based CI activities and acquire information systems and other technology-based tools for the CI Program.

(6) Conduct CI evaluations, to include CI-scope polygraph examinations, for covered persons in certain high risk programs.

e. Graded Protection. DOE will determine and allocate the level of CI resources to be applied based on the perceived level of risk posed to DOE information (e.g. classified, unclassified, proprietary, or unclassified controlled information), personnel, and assets from intelligence collection by or on behalf of foreign powers or entities, international terrorists, and insiders who engage in activities on behalf of these entities.

f. Site-Specific CI Support Plans. CI program plans will be tailored to address site-specific concerns and will be developed in coordination with OCI/ODNCI and the local or servicing CI office. Site-specific CI support plans should address the following areas at a minimum.

(1) Threat Analysis. Conduct an assessment of the threat from foreign intelligence collection and international terrorist activities tailored to the site and conduct ongoing analysis of the threat to support prioritization of local and national CI Program activities.

(2) Information Technology. Develop specific action plans to counter the threat to information systems posed by foreign intelligence collection and international terrorist activities.

(3) Awareness. Ensure that site management and personnel are aware of their responsibilities in support of the CI Program.

(4) Briefing and Debriefing. Brief and debrief personnel whose activities require foreign travel, hosting foreign visitors or assignees, or working in high-risk positions or special access programs or who otherwise need focused CI program support.

(5) Investigations and Inquiries. Conduct investigations and inquiries on matters of CI concern.

(6) Liaison. Interact with local law enforcement and the United States intelligence community (USIC) in support of the site CI Program.

(7) Unclassified Foreign Visits and Assignments (UFVA) Program Support. Coordinate UFVA matters in support of the site CI Program.

(8) Security Support. Coordinate with security program administrators on matters related to the site CI Program.

(9) Support the CI Evaluations Program. Conduct activities in support of CI evaluations of high-risk personnel as required by law and DOE regulations.

(10) Foreign Travel. Coordinate foreign travel matters in support of the site CI Program.

(11) Training. Address training needs of CI staff and CI Representatives and site staff on CI issues.

g. Program Appraisal and Assessment.

(1) DOE will strive for continuous CI Program improvement and will validate improvement using an internal inspection process.

(2) This internal inspection process will include reviewing CI programs and activities and making recommendations for improving program administration, effectiveness, and efficiency.

(a) The OCI Director will review and assess the CI Program regularly in accordance with established program requirements. To support these assessments, the Director and the ODNCI Chief will consult, as appropriate, with OCI program directors, site/facility managers, other DOE officials, and USIC and law enforcement officials with whom CI office personnel interact in the course of official business. For NNSA specific sites, assessments will be scheduled in coordination with the ODNCI Chief.

(b) Performance assessments may cover but are not limited to the following program dimensions and functional activities:

1 quality, quantity, and/or timeliness of investigations, actions recommended in accordance with such overriding requirements as referrals to the Federal Bureau of Investigation (FBI) under Section 811 of the Intelligence Authorization Act of 1995;

2 quality and effectiveness of CI program management (planning, organizing, directing/executing, budgeting, coordinating, communicating, evaluating, and quality assurance) in relation to resources, personnel, and operations;

3 quality and effectiveness of program components to include the integration of UFVA, awareness, briefing and debriefing, reporting, investigations, information and

special technologies, analysis, information management, financial management, liaison, training, evaluation program support, unique and/or high-risk personnel administration, and high-risk personnel evaluation;

4 compatibility of performance results with OCI/ODNCI policies, procedures, program directives, strategic planning, and other administrative requirements;

5 quality of data gathered, evaluated, recorded, and reported through CI briefings and debriefings of individuals who have professional, substantive personal, enduring, or financial contact with sensitive country foreign nationals;

6 program capability to define and counter CI risks and concerns resulting from DOE activities, especially those that involve interaction with foreign nationals for official and unofficial reasons;

7 quality, accuracy, and timeliness of CI work products submitted in response to requirements, assignments, or requests for support issued by the OCI Director or the ODNCI Chief;

8 quality of local CI program liaison and interaction with local FBI, USIC, and law enforcement personnel;

9 measures taken to identify and resolve matters of CI concern and promote proactive interaction, communications, and liaison with the site/facility manager, contract manager, and other operational elements (e.g., security, personnel administrators, export control, technology transfer, classified and unclassified computer security, foreign travel, and foreign visits and assignments).

(3) The OCI/ODNCI will maintain records of inspection scheduling, criteria, recommendations, and corrective actions for the Secretary and Administrator.

h. Local CI Office. The OCI Director/ODNCI Chief, in consultation with appropriate Secretarial officers and site/facility management, will establish local CI offices at specific sites and locations. Local CI offices will implement the CI Program at those sites/facilities and may also act as the servicing CI offices for additional DOE sites/facilities as designated by the OCI Director and the ODNCI Chief.

i. Servicing CI Office. Some local CI offices at DOE sites/facilities will be designated as servicing CI offices for additional facilities to support CI Program implementation at sites where it has been determined that a permanent local CI office is not required. Servicing CI offices will support implementation of a graded approach to the CI Program and efficient use of resources within the CI Program and supported sites/facilities.

j. Indices Checks.

(1) UFVAs involving terrorist- or sensitive-country nationals, sensitive subjects, and visits to security areas require that indices checks be requested 30 days before the first day of access.

(2) In rare cases when there is insufficient time to complete an indices check before the first day of access, the approval authority may request a CI consultation in lieu of the completing indices check for non-terrorist country nationals. Counterintelligence consultations may not be employed as a standard alternative to indices checks.

(3) Relief from the requirement to submit an indices check request 30 days in advance is provided to some sites for certain unclassified foreign national visits. This relief applies only to visits of 30 days or less and visits not involving sensitive subjects, security areas or visitors from terrorist-supporting countries. The relief does not apply to assignments.

5. RESPONSIBILITIES.

a. Secretary of Energy.

(1) Promulgates DOE CI policies for the Department, including the NNSA.

(2) Maintains an effective CI Program in accordance with E.O. 12333, the National Defense Authorization Act (NDAA) of 2000, and *DOE Procedures for Intelligence Activities* to ensure that the program—

(a) conducts CI activities to protect DOE information (e.g. classified, unclassified controlled information, proprietary, unclassified), personnel, and assets from intelligence collection by international terrorists or on behalf of foreign powers or entities and

(b) detects and deters efforts of insiders who engage in activities on behalf of a foreign intelligence service or international terrorist entity.

(3) Delegates non-NNSA management, implementation, and oversight responsibilities to the OCI Director.

(4) Delegates to a management panel consisting of the Director, Office of Security; Director, Office of Intelligence; and the Director, OCI, authority to approve access by foreign nationals who were born in, are citizens of, are employed by, or are representing entities in countries identified as state sponsors of terrorism.

(5) Authorizes the NNSA Administrator to delegate responsibility for implementing a CI Program for NNSA to the ODNCI Chief.

b. Administrator, NNSA.

(1) Establishes and maintains an effective CI Program in accordance with E.O. 12333, the NDAA of 2000, and *DOE Procedures for Intelligence Activities* to—

(a) implement CI Program policies for NNSA sites and facilities;

(b) conduct CI activities to protect NNSA information (e.g. classified, unclassified controlled information, proprietary, unclassified), personnel, and assets from intelligence collection by or on behalf of foreign powers or entities and international terrorist activities; and

(c) detect and deter insiders who engage in activities on behalf of a foreign intelligence service or international terrorist entity.

(2) Delegates CI Program implementation and related responsibilities to the ODNCI Chief.

c. Secretarial Officers.

(1) Support the implementation of an effective CI Program by providing program and project direction consistent with DOE-wide CI directives.

(2) In coordination with the OCI Director and the ODNCI Chief—

(a) ensure that adequate CI programs are established across the Department/Administration;

(b) support the OCI or ODNCI as appropriate in the development, review, and approval of site-specific CI support plans for each site under their purview;

(c) establish CI support programs for their respective Headquarters elements and designate CI Representatives for Headquarters organizations, as appropriate;

(d) ensure that contractors' requests for procurement requiring application of this Order incorporate requirements specified in the CRD of this Order;

(e) ensure that contracting officers for each site/facility are notified when site/facility management contractors are affected by requirements of this Order and ensure that the CRD is incorporated into affected site/facility management contracts;

(f) ensure that non-DOE-funded work under their jurisdiction is protected in accordance with applicable DOE CI directives; and

(g) support the establishment of local CI offices.

d. OCI Director and ODNCI Chief (jointly).

(1) Delegate day-to-day CI Program implementation to functional program directors and coordinate management of program priorities and activities.

(2) In consultation with the appropriate Secretarial officers and each site, facility, operations office, service center, director or manager within their respective jurisdictions, establish local CI offices to implement the CI Program in accordance with the provisions of this Order and other DOE directives and nationally mandated CI requirements.

(3) Designate senior CI officers (SCIOs) at site, facility, or operations office/service centers to manage the local CI offices.

(4) In consultation with the appropriate Secretarial officers and site, facility, and operations offices, or service center managers within their respective jurisdictions, designate servicing CI offices for facilities without local CI offices.

(5) In coordination with appropriate local field management, designate individuals to serve as counterintelligence representatives (CRs) at sites supported by servicing CI offices.

(6) Oversee the assignment of CI responsibilities and execution by servicing SCIOs in support of CI Program activities.

(7) Maintain liaison with the FBI and other law enforcement and intelligence agencies and programs regarding CI information, activities, and investigations in their respective areas.

(8) Coordinate the development, implementation, and maintenance of a joint OCI/ODNCI strategic plan to guide long-term CI program and budget planning.

(9) Ensure professional training development and continuing professional availability for CI personnel across the DOE complex.

(10) Establish and maintain training necessary for Departmental and Agency staff to ensure appropriate awareness and professional knowledge of CI issues for the conduct of the broader national security missions.

(a) The CI Training Academy (CITA) has been established as an independent element of the National Training Center (NTC) in Albuquerque, NM to support the Training and Awareness Program.

(b) The CITA's primary missions are designed to—

1 support the development of professional training for CI staff across the complex and

2 support the training of other departmental and agency staff for awareness and professional knowledge of CI issues as they relate to the Department's broader national security missions.

(c) The CITA will participate in the continued enhancement of the Department's/Administration's educational services capability for national security professionals.

(11) Ensure that the CI training program integrates the resources of the USIC into the CI Program for efficiency.

(12) Ensure that the DOE CI staffs maintain proficiency levels comparable to their USIC peers.

(13) Establish and maintain a records management system to support the OCI/ODNCI.

e. Director, OCI.

(1) Reports directly to the Secretary, with direct access to all Department officials and contractors.

(2) Establishes policy for CI programs and activities at Departmental facilities in accordance with E.O. 12333, Section 3204 of the National Defense Authorization Act and *DOE Procedures for Intelligence Activities* requirements to—

(a) conduct CI activities to protect DOE information (e.g. classified, unclassified controlled information, proprietary, unclassified),

personnel, and assets from intelligence collection activities by or on behalf of foreign powers or entities and international terrorist activities and

(b) detect and deter insiders who engage in activities on behalf of a foreign intelligence service or international terrorist entity.

(3) Issues policy directives for the CI Program, and manages and directs non-NNSA CI programs at Headquarters and in the field.

(4) Consults with the ODNCI Chief on policy formulation or changes and on interagency or National Security Council (NSC) policy matters.

(5) Coordinates policy development as necessary with the senior intelligence officer to ensure compliance with Executive orders, Director of Central Intelligence directives and *DOE Procedures for Intelligence Activities*.

(6) Manages and directs the DOE Counterintelligence Inspection and Polygraph programs.

(7) Manages and directs Headquarters staff, line element, and administrative support for the CI program, including maintaining the integrity of information management and classified CI databases.

(8) Provides information on the status and effectiveness of CI programs and activities at Departmental facilities to the Secretary, the Director of Central Intelligence, and the Director of the FBI on a regular basis and in answer to special requests.

(9) Issues DOE referrals (including all referrals originating from within NNSA) to the FBI pursuant to Section 811 of the Intelligence Authorization Act of 1995 [Title 50 United States Code (U.S.C.) 402(a)].

(10) Establishes policy on qualifying and credentialing of OCI/ODNCI personnel and manages the control, issuance, and use of CI credentials and shields.

(11) Supports UFVA activities as follows.

(a) Establishes and identifies CI policy and information requirements related to access by foreign nationals to DOE sites, programs, technologies, and information for inclusion in the UFVA Program.

(b) Provides advice to Headquarters approval authorities and supports field CI officers with guidance on foreign national access issues to consider in reviews.

(c) Ensures that local capability and expertise is available to provide effective CI advice to local approval authorities regarding access approval requests.

(d) Develops and provides CI awareness modules for UFVA training.

(e) Coordinates the external indices check process with the appropriate U.S. Government agencies.

(f) Documents and maintains DOE-wide information on requests for and completion of indices checks.

(g) Maintains separate, classified analytical databases to document foreign interaction at DOE sites.

(h) As a member of the Secretary's Headquarters Management Panel, reviews applications for nationals of state sponsors of terrorism visits.

(12) Establishes policy on CI briefings/debriefings for DOE personnel on official travel to countries where they intend to have or have had discussions with sensitive country foreign nationals regarding sensitive subjects. This would include travel known in advance to involve meetings with sensitive country foreign nationals or chance meetings where there are foreign nationals from sensitive countries in attendance.

(13) Establishes policy on, manages, and directs the CI Investigations and Operations Program to investigate and conduct inquiries on incidents of CI concern.

(14) Manages and directs CI investigations and inquiries in DOE.

(15) Manages and directs an internal CI inspection process to evaluate the efficiency and effectiveness of CI program elements and provides results to the Secretary and the Administrator, NNSA.

(a) Establishes policy for developing corrective actions, inspection findings and recommendations pertaining to DOE sites and scheduling and implementation of corrective actions.

(b) Coordinates with the ODNCI Chief and the Office of Independent Oversight and Performance Assurance inspection scheduling at NNSA sites to minimize overlapping inspections.

(c) Monitors corrective actions taken for inspection findings and recommendations at DOE and NNSA sites.

(16) Conducts CI information technology activities to—

(a) protect DOE information architecture,

(b) detect and deter technical attacks and threats posed by intelligence collection directed against DOE by hostile foreign intelligence and international terrorist elements, and

(c) develop and acquire information systems and other technology-based tools for the CI program.

(17) Conducts analyses of threat posed by foreign intelligence and international terrorist activities.

(18) Provides threat information to DOE management to support the protection of DOE personnel, information, facilities, and assets.

(19) Manages a CI evaluation program covering employees and applicants for employment who are undergoing CI assessments in connection with their placement or retention in high-risk positions as required by law and regulations.

(20) Develops CI Program security and classification management policies in concert with the Chief of ODNCI and coordinates these policies with the Office of Security and Office of Intelligence.

(21) Ensures that all existing and future DOE site/facility management contracts include CI program goals, objectives, and performance criteria.

(22) Supports contractor performance evaluation process for implementing the CI Program as it applies to DOE contract administration, award fee, and appraisal.

(23) Develops, manages, and executes the CI Program budget and is accountable for coordination, information processing, and presentation of the unified CI annual budget to the Chief Financial Officer, the Office of Management and Budget, and the Office of Central Intelligence community management staff. Coordinates this activity with the ODNCI Chief and coordinates the submission of the CI budget with the Director, Office of Intelligence.

(24) In coordination with the ODNCI Chief, develops integrating procedures to ensure timely responses to requirements set by the Chief Financial Officer.

(25) Ensures that information developed through CI Program activities is shared with appropriate program offices and the Office of Security, including information which may affect personnel, physical, and

information security or operations security (OPSEC); and technical surveillance countermeasure (TSCM) programs.

(26) Coordinates with the Director, Office of Intelligence, those activities that require senior intelligence officer review and approval (per *DOE Procedures for Intelligence Activities*.

(27) As the senior counterintelligence officer, reports questionable activities to the Inspector General, General Counsel, and the Director of the Office of Intelligence as the senior intelligence officer (per E.O. 12333, E.O. 12863, and *DOE Procedures for Intelligence Activities*).

f. Chief, ODNCI.

(1) Reports to the NNSA Administrator, with direct access to the Secretary and all other Department officials and contractors.

(2) Ensures that DOE CI policies are implemented within NNSA.

(3) Develops, implements, and manages CI Programs at NNSA Headquarters and field facilities in accordance with E.O. 12333 and *DOE Procedures for Intelligence Activities* requirements to—

(a) conduct CI activities to protect DOE/NNSA information (e.g. classified, unclassified controlled information, proprietary, unclassified), personnel, and assets from intelligence collection activities by or on behalf of foreign powers or entities and international terrorist activities and

(b) detect and deter insiders who engage in activities on behalf of a foreign intelligence service or international terrorist entity.

(4) In coordination with OCI Director, directs OCI Headquarters program in support of ODNCI activities.

(5) Manages and directs the ODNCI Headquarters staff, line elements, and administrative support functions of the CI Program, including all personnel, programs, and operations responsible to NNSA elements.

(6) Implements the CI briefing/debriefing program for personnel who interact with foreign nationals and/or may otherwise require focused CI Program support.

(7) Advises the NNSA Administrator on contractual activities impacting CI Program goals, objectives, and performance throughout NNSA.

(8) Ensures that all existing and future NNSA associated site/facility management contracts include CI program goals, objectives, and performance criteria.

(9) Coordinates with the OCI Director the scheduling NNSA facilities inspections to evaluate the efficiency and effectiveness of CI Program elements.

(10) For NNSA facilities, develops corrective actions for inspection findings and recommendations and schedules those actions to ensure that they are fully implemented, in coordination with the OCI Director.

(11) Forwards to the OCI Director information on matters requiring a referral pursuant to Section 811 of the Intelligence Authorization Act of 1995 [50 U.S.C. 402(a)] for NNSA and advises the OCI Director concerning similar referrals made by the Naval Criminal Investigative Service (NCIS) to the FBI regarding Naval Reactors facilities.

(12) Oversees, manages and/or directs CI investigations conducted by ODNCI offices and keeps the OCI Director informed of investigations.

(13) Supports the contractor performance evaluation process as it pertains to site/facility management contractors' implementation of the CI Program as part of NNSA contract administration, award fees, and appraisal provisions.

(14) Conducts CI Information Technology activities to—

(a) protect DOE/NNSA information architecture;

(b) detect and deter technical attacks and threats posed by foreign intelligence collection directed against DOE/NNSA by hostile foreign intelligence and international terrorist elements; and

(c) develop and acquire information systems and other technology-based tools for OCI/ODNCI personnel.

(15) Conducts analyses of the threat posed by foreign intelligence and international terrorist activities and provides threat information to DOE/NNSA management to support the protection of DOE/NNSA personnel, information, facilities, and assets.

(16) Ensures that information developed through CI program activities is shared with the NNSA Office of Defense Nuclear Security, including information that may affect personnel security, physical security, information security, OPSEC, and TSCM programs.

(17) Coordinates with the Director, Office of Intelligence activities that require the Director's review and approval (per *DOE Procedures for Intelligence Activities*).

(18) Reports all questionable activities to the Inspector General, General Counsel, and the Director, Office of Intelligence as the senior intelligence officer (per E.O. 12333, E.O. 12863 and *DOE Procedures for Intelligence Activities*).

(19) Supports UFVA.

(a) Ensures that CI policy and information requirements are adhered to for the approval and management of unclassified access approval for foreign nationals to NNSA sites, programs, technologies, and information for Office of Defense Nuclear Security.

(b) Provides advice to NNSA Headquarters approval authorities and supports field CI officers with guidance on foreign national access issues to consider in performing reviews.

(c) For NNSA sites/facilities, ensures that local capability and expertise are available to provide effective CI advice to local approval authorities regarding access approval requests.

(d) For NNSA sites/facilities, develops and provides CI awareness modules for UFVA training, as applicable.

(e) Supports the coordination of the external indices check process with the appropriate U.S. Government agencies.

(f) Supports the documentation and maintenance of DOE-wide information on requests for and completion of indices checks.

(g) Supports the CI Program in maintaining a separate, classified analytical database to document foreign interactions at DOE/NNSA sites.

(h) For NNSA sites/facilities, supports the NNSA Administrator in the approval process for nationals of state sponsors of terrorism visits in coordination with the Director, Office of Defense Nuclear Security; the OCI Director; the Director, Office of Security; the Director, Office of Intelligence; the Secretary; or the Secretary's management panel, as appropriate.

(20) Develops CI Program security and classification management policies in concert with the Director of OCI and coordinates these policies with the Office of Security and Office of Intelligence.

g. DOE/NSNA Field, Service Center, Site, Laboratory or Facility Managers, and the DOE Power Marketing Administrations.

(1) Support and adhere to all CI-related statutory and regulatory requirements, as well as DOE CI directives impacting DOE CI program requirements at their sites.

(2) Ensure implementation of DOE CI program requirements at their sites and provide support to—

(a) the local or servicing CI office in the development and implementation of site/facility specific CI support plans in accordance with paragraph 4f of this Order and

(b) the OCI Director and or ODNCI Chief in the identification and selection of individuals to serve as CI Representatives, as appropriate, to support local requirements.

(3) Maintain effective coordination with the OCI Director/ODNCI Chief on matters of CI interest.

(4) Provide the SCIO, local or servicing CI office personnel, and the CI Representative direct access to senior management.

(5) Ensure that the servicing or local CI office has appropriate access to all records, facilities, operational activities, security information, IT systems, and databases necessary to perform official duties.

(6) Coordinate with the OCI Director/ODNCI Chief to ensure the implementation of CI plans for each DOE special access program (SAP), including SAP CI threat assessments.

(7) Provide support and assistance for CI eligibility evaluations and CI scope polygraphs for designated DOE high-risk personnel pursuant to statutory provisions and regulatory requirements [see Title 10 Code of Federal Regulations (CFR) Part 709, Polygraph Examination Regulation].

(8) Ensure the implementation of effective CI awareness programs for employees that include—

(a) initial and comprehensive briefings on CI,

(b) annual refresher briefings, and

(c) awareness briefings and training for specific employee groups as identified in site-specific awareness plans.

NOTE: Portions of the awareness program may be coordinated with the security awareness program at the discretion of local site officials.

(9) Institute and maintain processes for coordinating adverse personnel actions (disciplinary suspensions, terminations, involuntary separations, and revocations/reinstatements of access authorizations/security clearances) with the responsible local or servicing CI office.

(10) Ensure that CI resources are actively used to protect and preserve classified and/or sensitive programs and operations.

(11) Maintain accountability to both the Secretary and the NNSA Administrator, as appropriate, for the performance of CI Program functions and requirements at their locations.

(12) Use performance evaluation information provided by DOE/NNSA Headquarters to support performance appraisals of site/facility management contractors under their purview.

(13) Provide timely, thorough support to Headquarters CI organizations, taskings, and requests for information.

(14) Support the CI Program in assessing risks associated with sensitive country foreign visits and assignments and visits and assignments involving sensitive subjects or security areas by—

(a) supporting effective implementation of the local UFVA program,

(b) providing recommendations for approval/disapproval of specific visits,

(c) supporting the conduct of indices checks by the CI Program, and

(d) supporting briefings and debriefings conducted by the CI Program.

(15) Ensure that all employees are aware of the requirement to report the following to the local or servicing CI office.

(a) Official foreign travel to sensitive countries regardless of whether the traveler possesses a security clearance.

(b) Travel to countries where they intend to have or have had discussions with sensitive country foreign nationals regarding

sensitive subjects. This would include travel known in advance to involve meetings with sensitive country foreign nationals or chance meetings where there are foreign nationals from sensitive countries in attendance.

(c) All travel to any country when areas determined to be sensitive subjects will be discussed.

(d) Any substantive professional, substantive personal, or substantive or enduring financial relationships (see paragraph 6, Definitions) with foreign nationals affiliated with sensitive countries.

(e) Any contacts with foreign nationals who make requests that could be attempts at exploitation or elicitation. Examples are—

1 requests for documents or information that is viewed by the traveler as unexpected or unrelated to the purpose of the interaction;

2 requests for the traveler to transport back to the U.S. any package(s) or letter(s) for mailing in the U.S.;

3 requests of any kind that cause the traveler to feel uncomfortable or call into question the purpose of the request;

4 professional contacts and relationships with sensitive country foreign nationals, whether they occur at one's worksite or abroad; and

5 any foreign travel for which foreign monetary support is provided, whether to a sensitive or a non-sensitive country.

(f) Requests for unauthorized access to classified or otherwise sensitive information.

(16) At the discretion of the local or servicing CI office, support the briefing and debriefing of employees when—

(a) they travel to foreign countries, regardless of whether they hold security clearances;

(b) they host both sensitive and non-sensitive country foreign visitors and assignees who are going to be given access to sensitive subjects or security areas; and

(c) other circumstances arise which may warrant the briefing and debriefing of certain employees to support the CI Program.

(17) Support the proactive integration and use of information security and intrusion detection resources and capabilities to protect DOE/NNSA information architecture and deter and prevent technical attacks and other threats posed by foreign intelligence activities directed against DOE/NNSA by hostile foreign intelligence collection and international terrorist elements.

(18) Support analyses of the threat posed by foreign intelligence and international terrorist activities and provide threat information to DOE/NNSA management to support the protection of DOE/NNSA personnel, information, facilities, and assets.

(19) Support investigations and inquiries on incidents of CI concern.

h. Director, Office of Security.

(1) Provides DOE/NNSA CI Federal and contractor personnel access to appropriate security records and files throughout the DOE complex as needed to conduct CI activities in accordance with this Order and applicable laws, regulations, Executive orders, and other DOE directives.

(2) Ensures that Office of Security managers and personnel promptly refer to the OCI Director, the ODNCI Chief, or field CIOs information of CI concern identified in the standard course of fulfilling Office of Security mission requirements. This includes security incidents having foreign nexus implications or involving hostile foreign intelligence collection or international terrorist activity or incidents which may indicate deliberate compromise of classified information or technical penetration of DOE facilities.

(3) With the OCI Director and ODNCI Chief reviews matters pertaining to hostile foreign intelligence collection and international terrorist activities to ensure a coordinated assessment of and response to threats. This includes collaborating as necessary—

(a) design basis threats;

(b) OPSEC vulnerability assessments;

(c) technical surveillance countermeasures activities;

(d) security and counterintelligence awareness programs; and

(e) personnel security, information security, and protection operations.

(4) In cooperation with the OCI Director, coordinates the UFVA program and policies in accordance with DOE O 142.3, *Unclassified Foreign Visits and Assignments*, dated 6-18-04, to support CI Program implementation.

i. Associate Administrator for Defense Nuclear Security.

(1) Provides DOE/NNSA CI Federal and contractor personnel access to appropriate records and files throughout the DOE complex as needed to conduct CI activities in accordance with this Order and applicable laws, regulations, Executive orders, and other DOEdirectives.

(2) Ensures that Office of Defense Nuclear Security managers and personnel promptly refer to the OCI Director, the ODNCI Chief, or field CI personnel any information of CI concern that is identified in the standard course of fulfilling Office of Defense Nuclear Security mission requirements. This includes any security incidents having foreign nexus implications or involving threats from hostile foreign intelligence collection or international terrorist activity or incidents which may indicate deliberate compromise of classified information or technical penetration of DOE facilities.

(3) With the OCI Director and ODNCI Chief reviews matters pertaining to hostile foreign intelligence collection and international terrorist activities to ensure a coordinated assessment of and response to threats. This includes collaborating as necessary—

(a) design basis threats;

(b) OPSEC vulnerability assessments at applicable sites/facilities

(c) TSCM activities at NNSA sites/facilities

(d) security and counterintelligence awareness programs at NNSA sites/facilities, and

(e) personnel security, information security, and protection operations.

(4) With the ODNCI Chief coordinates UFVA programs and policies in accordance with DOE O 142.3, *Unclassified Foreign Visits and Assignments*, dated 6-18-04, and supports CI Program implementation.

j. Director, Office of Intelligence.

(1) Acts as the senior intelligence officer for DOE and oversees the Department's intelligence activities pursuant to E.O. 12333.

(2) Provides for and/or coordinates the gathering of foreign intelligence information for OCI/ODNCI Headquarters and field elements.

(3) Coordinates CI matters with the OCI Director/ODNCI Chief.

(4) Coordinates with the OCI Director/ODNCI Chief the dissemination of CI threat information.

(5) Supports OCI/ODNCI responsibilities to analyze, produce, and disseminate threat related CI information.

(6) Coordinates with the OCI Director/ODNCI Chief on the development of the DOE/NNSA portion of the National Foreign Intelligence Program (NFIP) budget.

k. Deputy Administrator for Naval Reactors. Ensures that all activities at joint NNSA-Navy sites involving CI interests are conducted in accordance with current specific agreements among ODNCI, the Department of the Navy, NCIS, the Office of Naval Reactors, and E.O. 12344, *Naval Nuclear Propulsion Program.*

l. Local/Servicing CI Office Senior Counterintelligence Officers.

(1) Implement the CI Program and related policies, standards, and guidelines pursuant to legal and regulatory mandates, provisions of this Order, DOE CI directives and other requirements.

(2) Ensure that site-specific CI support plans are developed in accordance with paragraph 4f of this Order for sites/facilities for which the local/servicing CI office is responsible.

(3) Serve as primary CI advisors and provide CI support to DOE/NNSA site/facility management in accordance with established local/servicing CI office areas of responsibility while maintaining concurrent accountability to the OCI Director/ODNCI Chief for fulfilling CI Program requirements.

(4) Pursuant to Section 811 of the Intelligence Authorization Act of 1995, immediately forward to the OCI Director/ODNCI Chief for referral by the OCI Director to the FBI any information, regardless of origin, which indicates that classified information is being or may have been disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.

(5) Establish and/or maintain records management systems that support local/servicing CI offices, in coordination with the OCI Director/ODNCI Chief.

(6) Notify OCI/ODNCI of all incidents of CI concern involving suspected or identified foreign intelligence or international terrorism activities, as well as suspected or identified technical penetrations affecting persons or facilities under their jurisdiction, and document these in appropriate CI information systems.

(7) Implement CI briefing/debriefing programs for personnel who travel to sensitive countries or interact or have contact with foreign nationals, pursuant to CI Program policy and under the direction of the OCI Director/ODNCI Chief.

(8) Support CI analyses of threats posed to sites/facilities by foreign intelligence and international terrorist activities and provide relevant threat information to CI investigative, training and awareness, and Information and Special Technology Program (ISTP) personnel and outside offices such as those involved in the execution of the foreign visits and assignments process and other national security-related duties.

(9) Ensure the proactive integration and use of information security and intrusion detection capabilities to protect DOE/NNSA information architecture and to detect and deter technical attacks and intelligence gathering activities directed against DOE/NNSA by hostile foreign intelligence and international terrorist elements.

(10) Ensure entry of all CI-relevant data into CI-Net applications, including the results of debriefings, analyses, cyber and liaison incident reports, and other lead information supplied by DOE or United States CI community.

(11) Conduct liaison with site counterparts (e.g., security, intelligence, export control, technology transfer, TSCM, OPSEC, and nonproliferation personnel) on national security matters.

(12) Conduct liaison with local, state, and Federal intelligence community and law enforcement agencies concerning CI matters and maintain complete records of these interactions.

(13) Execute OCI/ODNCI mission and related strategic plan requirements to detect and deter foreign intelligence collection activities and unauthorized personnel from compromising DOE assets (i.e., information, classified and unclassified computers).

(14) Support Headquarters OCI/ODNCI requests for information and assistance for other CI activities as deemed appropriate by the OCI Director/ODNCI Chief.

(15) Support and assist the CI Evaluation Program covering designated DOE high-risk personnel as required by current statutory provisions and related regulatory requirements (see 10 CFR Part 709).

(16) Ensure that the implementation of an effective CI awareness program for employees includes—

(a) initial and comprehensive briefings on CI,

(b) annual refresher briefings to reinforce and update awareness of CI issues and employee responsibilities, and

(c) additional awareness briefings and training for specific employee groups as identified in site-specific awareness plans.

NOTE: Portions of the awareness program may be conducted in conjunction with the security awareness program at the discretion of local site officials.

(17) Ensure that CI personnel receive professional training and development necessary to execute their duties in support of the CI mission and OCI/ODNCI strategic plan.

(18) Ensure coordination with the local supporting security, human resources or other organizational entity to institute and maintain a process for coordinating adverse personnel actions (e.g., disciplinary suspensions, terminations, involuntary separations, and revocations/reinstatements of access authorizations/security clearances).

(19) Implement local programs to assess CI concerns associated with foreign visitors and assignees and foreign travel.

(20) Ensure that CI resources are actively used to protect and preserve classified and/or sensitive programs and operations. Focus will be prioritized on programs with subject matter, personnel, or activities believed to be of hostile foreign intelligence collection or international terrorist interest, where the possible loss of classified or sensitive information and materials imposes substantive national security concerns, and where there is significant interaction with sensitive country foreign nationals.

(21) Support the evaluation of sensitive country foreign nationals' visits and assignments, and foreign visits and assignments involving sensitive subjects or security areas, including recommendations for approval/disapproval, background checks, and CI briefings and debriefings for hosts.

(22) Work in close cooperation with contractor CI personnel.

(23) Provide UFVA support.

(a) Review requests for foreign national access approval (e.g., visits involving information and technologies that are releasable to the public) and requests for designation of optional areas within property protection areas without sensitive information for CI and counterterrorism implications.

(b) At the request of a local hosting site, provide CI consultations to the approval authority and his or her designees to evaluate foreign national access in the absence of the required completed indices check, and document that the consultation was conducted in the Foreign Access Central Tracking System.

(c) Conduct briefings and debriefings of hosts/sponsors/escorts of foreign visitors and assignees and develop and provide CI awareness modules for local UFVA training.

(d) Coordinate the external indices check process for local sites.

(e) Document foreign interactions at local sites in the applicable databases.

(f) Support the approval process for nationals of state sponsors of terrorism visits in coordination with the OCI Director.

(24) Support CI activities for IT to—

(a) protect the DOE information architecture,

(b) detect and deter technical attacks and intelligence collection directed against DOE by hostile foreign intelligence and international terrorist elements, and

(c) develop and acquire information systems and other technology-based tools for the CI program.

(25) Support analyses of the threat posed by hostile foreign intelligence collection and international terrorist activities for CI purposes, and provide threat information to DOE management to support the protection of DOE personnel, information, facilities, and assets.

(26) Conduct investigations and inquiries on incidents of CI concern.

(27) Develop criteria and establish a process to identify and document site-specific unique access programs, positions and individuals.

m. CI Representatives. Coordinate with assigned servicing CI office SCIOs and local site management the implementation of the local CI Program which includes assistance to the servicing CI office for the development of a site-specific CI support plan and support to servicing CI office investigations.

NOTE: CI Representatives will not conduct CI investigations independent of the servicing CI office. The servicing CI office will conduct investigations and may request the support of the CI Representative.

n. Contracting Officers will incorporate the CRD of this Order (Attachment 2) into affected site/facility management contracts via the laws, regulations, and DOE directives clause and upon notification that the Order is applicable to a procurement action.

o. DOE Federal Employees.

(1) Report substantive professional, business, or personal contacts and relationships with sensitive country foreign nationals to the local or servicing CI office or local CI Representative (see paragraph 6, Definitions).

(2) Follow established procedures to notify local or servicing CI offices of impending official or unofficial travel to sensitive countries or to any foreign country for discussions involving sensitive subjects so that they may receive CI awareness briefings to mitigate potential risks and help prepare them for their visits.

(3) On return from official or unofficial travel, cooperate in CI debriefings to gather information about experiences that may be helpful to future travelers and to assist in ongoing analyses of CI vulnerabilities and threats.

(4) Notify the local or servicing CI office of foreign travel, whether to a sensitive country or not, for which substantive foreign monetary support is provided.

(5) As hosts for sensitive and non-sensitive country visitors and assignees who will be given access to sensitive subjects or security areas, maintain availability for pre- and post-visit or assignment briefings/debriefings by the local or servicing CI office.

(6) Report to the local or servicing CI office information concerning any approach or contact by an individual, regardless of nationality, attempting to acquire unauthorized access to sensitive or classified information or materials; attempts to commit espionage, sabotage, or terrorist acts against the United States; or any deliberate or foreign related incident/action regarding the loss, compromise, or suspected compromise of classified information.

6. DEFINITIONS.

a. Counterintelligence (CI)—the information gathered and activities conducted to protect against espionage or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs.

b. CI Employee—any full-time or part-time Federal or contractor employee who is designated by the OCI Director or the ODNCI Chief as having CI Program responsibilities that require participation in and/or access to sensitive CI matters, databases, and/or records.

c. CI Evaluation—the process, including a CI scope polygraph examination, employed by the Office of Counterintelligence to determine whether DOE Federal and contractor employees, other individuals assigned or detailed to Federal positions at DOE, or applicants for employment will be recommended for initial or continued access to high-risk positions, pursuant to required statutory provisions and related regulatory requirements embodied in DOE regulations at 10 CFR Part 709.

d. CI Indicator—information that reflects possible foreign intelligence or international terrorist motives/involvement/activity.

e. CI Investigation—administrative fact-finding and information gathering conducted by the DOE Office of Counterintelligence/NNSA Office of Defense Nuclear Counterintelligence to determine whether national security is being threatened and/or damaged by activities perpetrated against DOE personnel, information, activities, facilities, and technologies or systems by or on behalf of foreign powers, organizations or persons, or international terrorist organizations.

f. CI Officer (CIO)—a Federal or contractor employee appointed by the OCI Director/ODNCI Chief to conduct investigative matters and various additional duties in support of the CI Program. CIOs normally report to a senior CIO who is responsible for a specific CI Program field office.

g. CI Polygraph Program—engagement in activities and processes for administering CI scope polygraph examinations pursuant to required statutory provisions and related regulatory requirements embodied in DOE regulations at 10 CFR Part 709.

h. CI Representative—an employee who is formally appointed by local site management to serve in a coordination role with the CI Program. CI Representatives will normally be appointed when there are no on-site CI program personnel and where a servicing CI office covers the facility. The CI Representative acts as the interface between a servicing CI office and the local site to support CI Program implementation at the site.

i. Elicitation— subtle extraction of information during an apparently normal and innocent conversation

j. Emotional Bonds—feelings of affection or emotional attachment in a relationship.

k. Enduring Relationship—one that has existed or is expected to exist for a substantial period of time (months or years).

l. Exploitation—the harmful, merely instrumental utilization or unfair advantage of an individual or his capabilities for one's own gain.

m. Foreign Intelligence—information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons but not including counterintelligence other than information on international terrorist activities.

n. Foreign Interest—any of the following:

(1) a foreign government or foreign government agency;

(2) any form of business enterprise organized under the laws of any country other than the United States or its possessions;

(3) any form of business enterprise organized or incorporated under the laws of the United States or a State or other jurisdiction within the United States that is owned, controlled, or influenced by a foreign government, agency, firm, corporation, or person; or

(4) any person who is not a U.S. citizen.

o. Foreign National—anyone who is not a U.S. citizen by birth or naturalization.

p. Foreign Nexus—specific indications that a DOE employee or contractor employee is or may be engaged in clandestine or unreported relationships with foreign powers, organizations or persons, or international terrorists, contacts with foreign intelligence services; or other hostile activities directed against DOE facilities, property, personnel, programs, or contractors by or on behalf of foreign powers, organizations or persons, or international terrorists.

q. High-Risk—programs, offices, and positions subject to the counterintelligence evaluation and polygraph examination provisions specified in DOE regulations at 10 CFR 709.

r. Insider—anyone with authorized, unescorted access to any part of DOE facilities and programs.

s. International Terrorism—the unlawful use of force or violence by a group or individual who has some connection to a foreign power or whose activities

transcend national boundaries against persons or property, for purposes of intimidating or coercing a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

t. Local CI Office—the location where the CI Program has established a full-time presence for the conduct of CI Program activities staffed by personnel assigned to the CI program.

u. National Nuclear Security Administration (NNSA) Facilities—the laboratories and facilities covered by NNSA: Los Alamos, Lawrence Livermore, and Sandia national laboratories; the Kansas City, Pantex, and Y-12 plants; tritium operation facilities at the Savannah River Site; the Nevada Test Site; and any other sites or facilities as designated by the Secretary in consultation with the NNSA Administrator (see P.L. 106-65).

v. Senior CI Officer (SCIO)—a Federal or contractor employee serving full-time in support of the CI program and responsible for the management of a specific CI program field office located within a specific facility or housed in a location that services a number of facilities. SCIOs are appointed by the OCI Director or the ODNCI Chief directly or in consultation with local management.

w. Servicing CI Office—local DOE CI offices staffed with full-time personnel and assigned responsibility for providing CI services to additional designated DOE facilities including those without full-time personnel and ensuring that all Departmental activities receive necessary CI services.

x. Substantive Relationship—one that is enduring and involves substantive sharing of personal information and/or the formation of emotional bonds.

y. Substantive Sharing (of personal information)—discussion of private information about oneself that one would not routinely share with strangers.

7. REFERENCES. The following references constitute the enabling legislation, memorandums, policies, and directives and guidance documents for DOE O 475.1.

a. DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, dated 6-18-04.

b. DOE O 551.1B, *Official Foreign Travel*, dated 8-19-03.

c. E.O. 12333, *United States Intelligence Activities*, December 4, 1981; implemented by *Department of Energy Procedures for Intelligence Activities* as approved by the Office of the Attorney General of the United States, October 19, 1992.

d. E.O. 12344, *Naval Nuclear Propulsion Program*, dated February 1, 1982.

e. E.O. 12958, *Classified National Security Information*, dated April 17, 1995.

f. E.O. 12968, *Access to Classified Information*, dated August 2, 1995.

g. Presidential Decision Directive (PDD)/NSC-12, *Security Awareness and Reporting of Foreign Contacts*, dated August 5, 1995.

h. PDD/NSC-61, *U.S. Department of Energy Counterintelligence Program* (U), dated February 11, 1998.

i. 10 CFR 709, Polygraph Examination Regulations.

j. Public Law (P.L.) 83-703, Atomic Energy Act of 1954, as amended.

k. P.L. 106-65, National Defense Authorization Act for Fiscal Year 2000.

l. P.L. 106-398, National Defense Authorization Act for Fiscal Year 2001.

m. P.L. 80-253, National Security Act of 1947, as amended by Title VIII of the Intelligence Authorization Act of 1995(P.L. 103-359).

n. Secretarial Policy Memorandum regarding governing the relationship between the DOE Office of Counterintelligence and the NNSA Office of Defense Nuclear Counterintelligence, dated January 19, 2001.

o. *Mapping the Future of the Department of Energy's Counterintelligence Program* (U), dated July 1998.

p. White House Memorandum, *Early Detection of Espionage and other Intelligence Activities* through the Identification and Referral of Anomalies, dated August 23, 1996.

q. *Department of Energy Procedures for Intelligence Activities* as approved by the Office of the Attorney General of the United States, dated October 19, 1992.

r. Office of Counterintelligence Memorandum, *Relief from Requirement to Conduct Indices Checks in Advance of Certain Visits*, dated January 10, 2001.

s. Delegation Order No. 00-020.00 to the Director of Intelligence, dated December 6, 2001.

8. CONTACT. Questions concerning this Order should be directed to the OCI at 202-586-5901. Questions regarding NNSA CI activities should be directed to ODNCI at 202-586-9018.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

PRIMARY DOE ORGANIZATIONS TO WHICH DOE O 475.1 IS APPLICABLE

Office of the Secretary
Departmental Representative to the Defense Nuclear Facilities Safety Board
Energy Information Administration
National Nuclear Security Administration
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Office of Economic Impact and Diversity
Office of Electric Transmission and Distribution
Office of Energy Assurance
Office of Energy Efficiency and Renewable Energy
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of Inspector General
Office of Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation/Chief Financial Officer
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security
Office of Security and Safety Performance Assurance
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 475.1, Counterintelligence Program

Regardless of the performer of the work, the contractor is responsible for compliance with the requirements of this Contractor Requirements Document (CRD). The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor will not unnecessarily or imprudently flow down requirements to subcontracts. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD to the extent necessary to ensure the contractor's compliance and only incur costs that would be incurred by a prudent person in the conduct of competitive business.

The purpose of the Department of Energy (DOE)/National Nuclear Security Administration (NNSA) Counterintelligence (CI) Program is to gather information and engage in activities that are designed to protect Departmental resources and personnel against espionage or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or international terrorist activities.

This CRD establishes CI requirements for DOE contractors, including NNSA contractors.

1. BACKGROUND. The Director of the DOE Office of Counterintelligence (OCI) or the Chief of the NNSA Office of Defense Nuclear Counterintelligence (ODNCI) consults with appropriate DOE field site/facility management within their respective jurisdictions to establish local CI offices with full-time Federal and contractor CI personnel who implement the CI Program.

   In addition, determinations are made concerning each local CI office as to whether it will act as a servicing CI office for facilities that do not have local CI offices. A CI office may service more than one field office or site. The OCI Director/ODNCI Chief, to support CI Program requirements, may change the scope of responsibility for each local CI office.

   For managing and operating contractors, when it is determined that no local CI office is required, a servicing CI office for that contract will be designated and the contractor will be required to support the requirements of the site-specific CI plan developed for that contract in coordination with the servicing CI office and the OCI Director or the ODNCI Chief, as appropriate. At facilities not requiring a local CI office, a servicing CI office will be designated. For facilities supported by a servicing CI office an individual at the serviced site will be designated by site/facility management as the on-site contractor CI Representative. This selection should be coordinated with the servicing CI office Federal or contractor SCIO and the OCI Director or the ODNCI Chief as appropriate. All contractor CI personnel are required to work in close cooperation with field and Headquarters Federal CI personnel.

The contractor must ensure that the senior CI officer (SCIO) reports directly to both site/facility senior management and either the OCI Director or the ODNCI Chief. The contractor CI Representative reports to the SCIO for CI matters only.

2. PROGRAM DIMENSIONS. Contractor CI Programs will be evaluated in accordance with performance assessments covering, but not limited to, the following program dimensions and functional activities:

a. quality, quantity, and timeliness of investigations, including actions recommended in accordance with such overriding requirements as referrals to the Federal Bureau of Investigation (FBI) [see Title 50 United States Code (U.S.C.) 402a];

b. quality and effectiveness of the CI program management process (planning, organizing, directing/executing, budgeting, coordinating, communicating, evaluating, and quality assurance activities conducted in relation to CI resources, personnel, and operations);

c. quality and effectiveness of program components such as unclassified foreign visits and assignments (UFVA), CI awareness/briefing and debriefing/reporting, investigations, information and special technologies, CI analysis, information management, financial management, liaison, training, CI Evaluations Program support, and administration of unique and/or high-risk personnel;

d. compatibility of performance results with OCI/ODNCI policies, procedures, program directives, strategic planning, and other administrative requirements;

e. quality of data gathered, evaluated, recorded, and reported through CI briefings and debriefings of those individuals having professional, substantive personal, enduring, or financial contact with sensitive country foreign nationals;

f. ability of the program to define and counter any CI risks and concerns incurred as a result of DOE activities, especially those that involve interaction with foreign nationals for official and unofficial reasons;

g. quality, accuracy, and timeliness of CI work products submitted in response to requirements, assignments, and/or requests for support issued by the OCI Director/ODNCI Chief;

h. quality of the local CI program's liaison and interaction with local FBI, United States intelligence community (USIC), and law enforcement personnel; and

i. measures taken to identify and resolve matters of CI concern, and promote proactive interaction, communications, and liaison with the site/facility manager, contract manager, and/or other operational elements (e.g., security, personnel administrators, export control, technology transfer, classified and unclassified computer security, foreign travel, and foreign visits and assignments).

3. CONTRACTOR REQUIREMENTS.

a. Contractors and subcontractors under their purview must support, adhere to, and implement all DOE CI Program requirements at their sites.

b. The contractor must ensure implementation of the following DOE CI Program requirements.

(1) Support the local assigned servicing CI office in the development and implementation of site/facility specific CI support plans in accordance with paragraph 3c(2) of this CRD.

(2) At sites where a local CI office is co-located, implement the CI Program directly through the local office.

(3) At sites that use a servicing CI office at another location, contractors will coordinate implementation with the assigned servicing CI office.

(4) Site/facility management contractors at sites assigned to act as servicing CI offices for other contractor facilities will be responsible for developing site-specific CI support plans and overall CI Program implementation through the Federal or contractor servicing SCIO in coordination with those assigned sites and the OCI Director/ODNCI Chief.

(5) Support the Director and or Chief in identifying and selecting individuals to serve as contractor SCIOs or CI Representatives.

(6) Maintain effective coordination with the OCI Director and the ODNCI Chief on matters of CI interest.

(7) Provide the Federal or contractor SCIO, local or servicing CI office personnel, and the contractor CI Representative with direct access to senior management.

(8) Ensure that the local or servicing CI office has appropriate access to all records, facilities, operational activities, security information, IT systems, and databases necessary to perform its official duties.

(9) Coordinate with the OCI Director and the ODNCI Chief to ensure the implementation of CI plans for each DOE special access program (SAP) and SAP CI threat assessments.

(10) Provide support and assistance for CI eligibility evaluations and CI scope polygraphs for designated DOE high-risk personnel pursuant to current statutes and the regulatory requirements [Title 10 Code of Federal Regulations (CFR) Part 709, Polygraph Examination Regulations].

(11) Ensure that the implementation of an effective CI awareness program for contractor employees includes the following.

(a) Initial, comprehensive briefings on CI. Briefing topics include but are not limited to overview of the foreign intelligence collection and international terrorist threat, espionage indicators, and reporting requirements.

(b) Annual refresher briefing. Refresher briefings should reinforce and update awareness of CI issues and their responsibilities, regardless of whether the employee holds clearances or not.

(c) Additional awareness briefings and training for specific employee groups as identified in site-specific awareness plans.

NOTE: Portions of the awareness program may be coordinated with the security awareness program at the discretion of local site officials.

(12) Institute and maintain a process for coordinating adverse personnel actions with the responsible local or servicing CI office (including such actions as disciplinary suspensions, terminations, involuntary separations, and revocations/reinstatements of access authorizations/security clearances).

(13) Ensure that CI resources are used to protect and preserve classified and/or sensitive programs and operations.

(14) Maintain accountability to both the Secretary and the Administrator for the performance of CI program functions and requirements at their locations.

(15) Provide timely and thorough support to Headquarters CI Program Directors, CI taskings, and requests for information.

(16) Support the CI role in assessing risks associated with sensitive country foreign visits and assignments and or when sensitive subjects will be discussed or security areas will be used at DOE facilities by—

(a) supporting the effective implementation of the local UFVA program,

(b) providing recommendations for approval/disapproval of specific visits,

(c) supporting the conduct of indices checks by the CI Program, and

(d) supporting the conduct of briefings and debriefings by the CI Program.

(17) Ensure that all contractor employees are aware of the requirement to report the following to the local or servicing CI office.

(a) Official foreign travel to sensitive countries regardless of whether the traveler possesses a security clearance.

(b) Travel to any country where they intend to have or have had discussions with sensitive country foreign nationals regarding sensitive subjects. This would include travel which they know in advance will involve meetings with sensitive country foreign nationals or chance meetings where there are foreign nationals from sensitive countries in attendance.

(c) All travel to any country when areas determined to be sensitive subjects will be discussed.

(d) Any substantive professional, personal, or enduring financial relationship [one that has existed, or is expected to exist, for a substantial period of time (months or years)] with foreign nationals affiliated with sensitive countries.

(e) Any contacts with foreign nationals who make requests that could be attempts at exploitation or elicitation. Examples are—

1 requests for documents or information that is viewed by the traveler as unexpected or unrelated to the purpose of the interaction;

2 requests for the traveler to transport back to the U.S. any package(s) or letter(s) for mailing in the U.S.;

3 requests of any kind that cause the traveler to feel uncomfortable or call into question the purpose of the request;

4 professional contacts and relationships with sensitive country foreign nationals, whether they occur at one's worksite or abroad; and

5 any foreign travel for which foreign monetary support is provided, whether to a sensitive or a non-sensitive country.

(f) Requests for unauthorized access to classified or otherwise sensitive information.

(18) At the discretion of the local or servicing CI office, support the briefing and debriefing of contractor employees when warranted to support the CI Program, including contractor employees who are—

(a) traveling to sensitive foreign countries when required regardless of whether they hold a security clearance or

(b) hosting sensitive and non-sensitive country foreign visitors and assignees that are going to be given access to sensitive subjects or sites.

NOTE: Other circumstances may arise which could warrant the briefing and debriefing of certain employees to support the CI Program.

(19) Support the proactive integration and use of information security and intrusion detection resources and capabilities to protect the DOE information architecture and detect and deter technical attacks and intelligence collection directed against DOE by hostile foreign intelligence and international terrorist elements.

(20) Support analyses of the threats posed by foreign intelligence services and international terrorist activities for CI purposes and provide threat information to DOE management to support the protection of DOE personnel, information, facilities, and assets.

(21) Support the conduct of investigations and inquiries about incidents of CI concern.

c. The contractor must ensure that the assigned SCIO performs the following functions at the local site and for assigned sites which they service. For sites not assigned a local SCIO, the assigned servicing CI office SCIO will be responsible for performing these same functions in coordination with the local contractor site contractor CI Representative.

(1) Implement CI Program policies, standards, and guidelines pursuant to legal and regulatory mandates, provisions of this Order, and other relevant DOE CI directives and requirements.

(2) Ensure the development of a site-specific CI support plan for each site/facility for which the local/servicing CI office is responsible. These plans are to be developed in coordination with OCI/ODNCI, as appropriate. Site specific CI support plans should address the following areas at a minimum.

(a) Threat Analysis. Conduct site-based counterintelligence threat assessments based on a variety of sources, including foreign intelligence and international terrorist information. Conduct

ongoing analysis of the threat to support prioritization of local and national CI Program activities.

(b) Information Technology. Develop specific actions to be taken to counter the threat to information systems posed by foreign intelligence collection and international terrorist activities.

(c) Awareness. Ensure site personnel are aware of their responsibilities to support the CI Program.

(d) Briefing and Debriefing. Brief and debrief specific personnel whose activities require foreign travel, hosting foreign visitors or assignees, working in high risk positions or special access programs or who otherwise need focused CI program support.

(e) Investigations and Inquiries. Conduct investigations and inquiries on matters of CI concern.

(f) Liaison. Conduct liaison with local law enforcement and the USIC in support of the site CI Program.

(g) UFVA support. Coordinate the UFVA matters.

(h) Security support. Coordinate with security on matters related to the site CI Program.

(i) Support to the CI Evaluation Program. Conduct activities in support of CI evaluations of high risk personnel as required by law and DOE regulations (10 CFR 709).

(j) Foreign Travel. Coordinate on foreign travel matters in support of the site CI Program.

(k) Training. Address training needs of the CI staff, CI Representatives, and site staff on CI issues, as appropriate.

(3) Serve as the primary CI advisor and provide CI support to DOE site/facility management in accordance with established local/servicing CI office areas of responsibility while maintaining concurrent accountability to the OCI Director/ODNCI Chief for fulfilling CI Program requirements.

(4) Immediately forward to the OCI Director/ODNCI Chief for referral by the OCI Director to the FBI, any information, regardless of origin, which indicates that classified information is being or may have been disclosed in an unauthorized manner to a foreign power or an agent of a foreign power (see 50 U.S.C. 402a).

(5) Establish and/or maintain an approved records management system to support the local/servicing CI office, in coordination with the OCI Director/ODNCI Chief.

(6) Notify OCI/ODNCI of all incidents of CI concern involving suspected or identified hostile foreign intelligence or international terrorism activities and suspected or identified technical penetrations affecting persons or facilities under their jurisdiction and document these in appropriate CI information systems, as applicable.

(7) Implement a CI briefing/debriefing program for contractor personnel who travel to a sensitive country or interact or have contact with foreign nationals, pursuant to CI Program policy and under the direction of the OCI Director/Chief ODNCI.

(8) Conduct analyses to assess the threats posed by foreign intelligence services and international terrorist activities to sites/facilities for CI purposes and provide relevant threat information to CI investigative, training and awareness, and Information and Special Technology Program (ISTP) personnel and outside offices such as those involved in foreign visits and assignments and other national security–related duties.

(9) Ensure the proactive integration and use of information security and intrusion detection capabilities to protect the DOE information architecture and to detect and deter technical attacks and intelligence gathering activities directed against DOE by foreign intelligence and international terrorist elements.

(10) Ensure entry of all CI-relevant data into existing CI-Net applications, (or successor systems), including the results of investigations, debriefings, analysis, cyber, liaison, incident reports, and other lead information supplied by the DOE CI community.

(11) Conduct liaison with site counterparts (including security, intelligence, export control, technology transfer, technical surveillance countermeasures, operations security, and nonproliferation personnel) on national security matters.

(12) Conduct liaison with appropriate local, state, and Federal intelligence and law enforcement agencies, as appropriate, concerning CI/counterterrorism matters and maintain a complete record of these interactions.

(13) Execute OCI/ODNCI mission and related strategic plan requirements to deter, detect, and prevent foreign powers and other unauthorized personnel from compromising DOE assets (e.g., information or classified and unclassified computers).

(14) Support Headquarters OCI/ODNCI, including Program Directors, requests for information and assistance for other CI activities as required and deemed appropriate by the OCI Director or the ODNCI Chief.

(15) Support and assist the CI Evaluation Program covering designated DOE high risk personnel, as required (10 CFR Part 709).

(16) Ensure the implementation of an effective CI awareness program for contractor employees that includes the following.

(a) Initial briefings on CI. Briefing topics include but are not limited to overview of the foreign intelligence collection and international terrorist threat, espionage indicators, and reporting requirements.

(b) Annual refresher briefings. Refresher briefings should reinforce and update awareness of CI issues and employees' responsibilities, regardless of whether they hold clearances or not.

(c) Additional awareness briefings and training for specific employee groups as identified in site-specific awareness plans

NOTE: Portions of the awareness program may be coordinated with the security awareness program at the discretion of local site officials.

(17) Ensure that subordinate CI contractor personnel, including CI Representatives, receive the professional training and development necessary to execute their particular duties in support of the overall CI mission and OCI/ODNCI Strategic Plan.

(18) Ensure coordination with the local supporting security, human resources, or other organizational entity to institute and maintain a process for coordinating adverse personnel actions (including such actions as disciplinary suspensions, terminations, involuntary separations, and revocations/reinstatements of access authorizations/security clearances).

(19) Implement local programs to assess CI implications of foreign visitors and assignees and foreign travel.

(20) Ensure that CI resources are actively used to protect and preserve classified and/or sensitive programs and operations. Focus will be prioritized on programs with subject matter, personnel, or activities believed to be of interest to hostile foreign intelligence or international terrorist entities, where the possible loss of classified or sensitive information and materials imposes substantive national security concerns, and where there is significant interaction with sensitive country foreign nationals.

(21) Support the evaluation of sensitive foreign country foreign visits and assignments to DOE facilities, including recommendations for approval/disapproval, the conduct of indices checks, and the conduct of host CI briefings and debriefings.

(22) Require contractor personnel to work in close cooperation with Federal CI personnel.

(23) Support the UFVA program.

(a) Review requests for foreign national access approval, including visits involving information and technologies that are releasable to the public, and requests for designation of optional areas within property protection areas for CI and Counterterrorism implications. This includes attendance in offsite conferences and other functions when foreign national access approval is required.

(b) At the request of the local hosting site, provide CI consultations to the approval authority and his or her designees to evaluate foreign national access in the absence of a required, completed indices check, and document that the consultation was conducted in the Foreign Access Central Tracking System.

(c) Conduct briefings and debriefings of foreign visitors' and assignees' hosts/sponsors/escorts and develop and provide CI awareness modules for local UFVA training.

(d) Coordinate the external indices check process for local sites.

(e) Document foreign interaction at the local site in applicable databases.

(f) Support as required the approval process for nationals of state sponsors of terrorism visits in coordination with the OCI Director.

(24) Support the conduct of information technology CI activities to protect the DOE information architecture; to detect and deter technical attacks and intelligence collection directed against DOE by hostile foreign intelligence and international terrorist elements; and to develop and acquire information systems and other technology-based tools for the CI program.

(25) Support analyses of the threat posed by foreign intelligence and international terrorist activities for CI purposes and provide threat information to DOE management to support the protection of DOE personnel, information, facilities, and assets.

(26) Support investigations and inquiries on incidents of CI concern.

(27) Develop criteria and establish a process to identify and document site-specific unique access programs, positions and individuals.

d. Contractor CI Representatives will be appointed by site/facility managers, in coordination with the servicing SCIO and the OCI Director/ODNCI Chief for sites supported by a servicing CI office. For CI purposes only, contractor CI Representatives will report directly to their servicing CI office Federal or contractor SCIO. The contractor CI Representative position is not intended to be a full time responsibility.

(1) Contractor CI Representatives will coordinate with the assigned servicing CI office Federal or contractor SCIO and local site management on the implementation of the local CI Program. This will include at a minimum assistance to the servicing CI office for the development of a site-specific CI support plan.

(2) Contractor CI Representatives will support the servicing CI office in the conduct of investigations.

NOTE: The CI Representative will not conduct CI investigations independent of the servicing CI office. The servicing CI office will conduct investigations and may request the support of the local contractor CI Representative, as appropriate.

4. DEFINITIONS.

a. Counterintelligence (CI)—the information gathered and activities conducted to protect against espionage or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs.

b. CI Employee—any full-time or part-time Federal or contractor employee who is designated by the OCI Director or the ODNCI Chief as having CI Program responsibilities that require participation in and/or access to sensitive CI matters, databases, and/or records.

c. CI Evaluation—the process, including a CI scope polygraph examination, employed by the Office of Counterintelligence to determine whether DOE Federal and contractor employees, other individuals assigned or detailed to Federal positions at DOE, or applicants for employment will be recommended for initial or continued access to high-risk positions, pursuant to required statutory provisions and related regulatory requirements embodied in DOE regulations at 10 CFR Part 709.

d. CI Indicator—information that reflects possible foreign intelligence or international terrorist motives/involvement/activity.

e. CI Investigation—administrative fact-finding and information gathering conducted by the DOE Office of Counterintelligence/NNSA Office of Defense Nuclear Counterintelligence to determine whether national security is being threatened and/or damaged by activities perpetrated against DOE personnel, information, activities, facilities, and technologies or systems by or on behalf of foreign powers, organizations or persons, or international terrorist organizations.

f. CI Officer (CIO)—a Federal or contractor employee appointed by the OCI Director/ODNCI Chief to conduct investigative matters and various additional duties in support of the CI Program. CIOs normally report to a senior CIO who is responsible for a specific CI Program field office.

g. CI Polygraph Program—engagement in activities and processes for administering CI scope polygraph examinations pursuant to required statutory provisions and related regulatory requirements embodied in DOE regulations at 10 CFR Part 709.

h. CI Representative—an employee who is formally appointed by local site management to serve in a coordination role with the CI Program. CI Representatives will normally be appointed when there are no on-site CI program personnel and where a servicing CI office covers the facility. The CI Representative acts as the interface between a servicing CI office and the local site to support CI Program implementation at the site.

i. Elicitation— subtle extraction of information during an apparently normal and innocent conversation

j. Emotional Bonds—feelings of affection or emotional attachment in a relationship.

k. Enduring Relationship—one that has existed or is expected to exist for a substantial period of time (months or years).

l. Exploitation—the harmful, merely instrumental utilization or unfair advantage of an individual or his capabilities for one's own gain.

m. Foreign Intelligence—information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons but not including counterintelligence other than information on international terrorist activities.

n. Foreign Interest—any of the following:

(1) a foreign government or foreign government agency;

(2) any form of business enterprise organized under the laws of any country other than the United States or its possessions;

(3) any form of business enterprise organized or incorporated under the laws of the United States or a State or other jurisdiction within the United States that is owned, controlled, or influenced by a foreign government, agency, firm, corporation, or person; or

(4) any person who is not a U.S. citizen.

o. Foreign National—anyone who is not a U.S. citizen by birth or naturalization.

p. Foreign Nexus—specific indications that a DOE employee or contractor employee is or may be engaged in clandestine or unreported relationships with foreign powers, organizations or persons, or international terrorists, contacts with foreign intelligence services; or other hostile activities directed against DOE facilities, property, personnel, programs, or contractors by or on behalf of foreign powers, organizations or persons, or international terrorists.

q. High-Risk—programs, offices, and positions subject to the counterintelligence evaluation and polygraph examination provisions specified in DOE regulations at 10 CFR 709.

r. Insider—anyone with authorized, unescorted access to any part of DOE facilities and programs.

s. International Terrorism—the unlawful use of force or violence by a group or individual who has some connection to a foreign power or whose activities transcend national boundaries against persons or property, for purposes of intimidating or coercing a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

t. Local CI Office—the location where the CI Program has established a full-time presence for the conduct of CI Program activities staffed by personnel assigned to the CI program.

u. National Nuclear Security Administration (NNSA) Facilities—the laboratories and facilities covered by NNSA: Los Alamos, Lawrence Livermore, and Sandia national laboratories; the Kansas City, Pantex, and Y-12 plants; tritium operation facilities at the Savannah River Site; the Nevada Test Site; and any other sites or facilities as designated by the Secretary in consultation with the NNSA Administrator (see P.L. 106-65).

v. Senior CI Officer (SCIO)—a Federal or contractor employee serving full-time in support of the CI program and responsible for the management of a specific CI program field office located within a specific facility or housed in a location that services a number of facilities. SCIOs are appointed by the OCI Director or the ODNCI Chief directly or in consultation with local management.

w. Servicing CI Office—local DOE CI offices staffed with full-time personnel and assigned responsibility for providing CI services to additional designated DOE facilities including those without full-time personnel and ensuring that all Departmental activities receive necessary CI services.

x. Substantive Relationship—one that is enduring and involves substantive sharing of personal information and/or the formation of emotional bonds.

y. Substantive Sharing (of personal information)—discussion of private information about oneself that one would not routinely share with strangers.