U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5639.1

10/19/92

SUBJECT: INFORMATION SECURITY PROGRAM

---

1. PURPOSE. To establish the Department of Energy (DOE) Information Security Program and set forth policies, procedures and responsibilities for the protection and control of classified and sensitive information. The Information Security Program is a system of elements which serve to deter collection activities.

2. APPLICATION TO CONTRACTS. Except as excluded in paragraph 3, the provisions of this Order are to be applied to covered contractors and they will apply to the extent implemented under a contract or other agreement. A covered contractor is a seller of supplies or services involving access to classified or sensitive information, and awarded a procurement contractor subcontract.

3. EXCLUSION. DOE facilities and activities regulated by the Nuclear Regulatory Commission (NRC) are exempt from the requirements of this Order. Office of Civilian Radioactive Waste Management (RW) personnel and activities not directly associated with the NRC licensed facilities and thus not covered by the NRC directives are subject to the provisions of this Order.

4. REFERENCES. See Attachment 1.

5. DEFINITIONS. See Attachment 2.

6. POLICY.

   a. DOE's policy for protecting security interests applies equally to all organizations (Departmental Elements and contractors); however, site specific characteristics must be considered to assure that information is properly controlled. Site-specific procedures shall be documented in approved security plans.

   b. Individuals are responsible for protecting all classified and sensitive information to which they have access or custody.

   c. Classified information may only be disclosed to a contractor by a U.S. Government agency pursuant to an authorized and legitimate U.S. Government requirement. A contractor may not further disclose that information except to its appropriately cleared employees, subcontractors, and consultants who have a need-to-know in connection with the performance requirements of the contract under which it was received, without the specific authorization of the DOE program office that has jurisdiction over the information.

DISTRIBUTION:

All Departmental Elements

INITIATED BY:

Office of Safeguards and Security

d. Classified information shall not be released to the public until it has been formally and officially declassified by appropriate classification authority and its release is otherwise permitted by applicable law or regulation.

7. CONCEPT OF OPERATION. Information security addresses a program of measures to protect classified and sensitive information, including management and supervision, training, procedures, equipment and the integration of these elements. This Order sets forth the framework for the Orders in the 5639 series which define the policies and baseline requirements related to specific aspects of the Information Security Program. The Information Security Program encompasses the following major elements:

a. Classified matter protection and control (CMPC).

b. Violations of Laws, Losses, and Incidents of Security Concerns (VOLLI), to include unauthorized disclosures.

c. Unclassified Controlled Nuclear Information (UCNI).

d. Technical surveillance countermeasures (TSCM).

e. Automated information systems security (AISS).

f. Operations security (OPSEC).

g. Security of Foreign Intelligence Information (FII) and Sensitive Compartmented Information (SCI) Facilities (SCIF).

h. Official Use Only (OUO).

i. Foreign Ownership, Control, or Influence (FOCI).

j. Security of Special Access Programs (SAP).

Specific standards, procedures and requirements for the control of classified and sensitive information are contained in DOE Orders and other documents as referenced in Attachment 1.

8. RESPONSIBILITIES AND AUTHORITIES. Additional responsibilities and authorities are assigned within the individual 5639 series of safeguards and security Orders.

a. Secretarial Officers, in addition to responsibilities in 8b, shall:

(1) Ensure that information security programs are implemented for facilities and activities under their cognizance.

(2) Ensure that adequate resources are made available to implement and maintain the Information Security Program.

(3) Ensure that information security is included in protection program planning documents.

(4) When required, appoint a team to conduct damage assessments and an individual to conduct initial inquiries regarding unauthorized disclosures and unaccounted-for classified and sensitive matter.

(5) Approve completed reports of damage assessments and provide the assessment reports to SA-1.

b. Heads of Departmental Elements shall:

(1) Establish security organizations which are staffed with knowledgeable individuals and provide adequate resources.

(2) Ensure that information security is included in protection program planning documents.

(3) Develop and approve procedures which address information security.

(4) Ensure compliance with security procedures for the control and Protection of classified and sensitive information in accordance with the provisions of DOE Orders.

(5) Ensure that an effective program is instituted for the protection and control of classified matter and that access to classified and sensitive information is authorized on a need-to-know basis.

(6) Develop education and training programs to ensure that individuals are aware of their responsibilities to protect and control classified and sensitive information. Ensure that minorities, women and persons with disabilities are accorded equal opportunity to receive training.

(7) Ensure individuals who prepare and handle classified and sensitive matter are given appropriate training in protection and control procedures consistent with Departmental policies.

(8) Ensure security activities are registered for programs requiring classified information control in accordance with DOE 5634.1B, FACILITY APPROVALS, SECURITY SURVEYS AND NUCLEAR MATERIAL SURVEYS, of 9-15-92.

(9) Submit reports of unauthorized disclosures of classified information to SA-1 immediately.

(10) Ensure disciplinary and corrective action are taken as a result of infractions and ensure records of security infractions are maintained.

(11) Establish a self-assessment program for information security.

(12) Designate an individual (s) to be responsible for bringing to the attention of the contracting officer each procurement falling within the scope of this Order. Unless another individual is designated, the responsibility is that of the procurement request originator (the individual responsible for initiating a requirement on DOE F 4200.33, "Procurement Request Authorization"):

(13) Ensure that contractors:

(a) Develop, implement, and manage a comprehensive information security program in accordance with the provisions of this Order.

(b) Establish security organizations which are staffed with knowledgeable individuals and provide adequate resources.

(c) Ensure that information security is included in protection program planning documents.

(d) Develop procedures which address information security.

(e) Ensure compliance with security procedures for the control and protection of classified and sensitive information in accordance with the provisions of DOE Orders.

(f) Ensure that an effective program is instituted for the protection and control of classified matter and that access to classified and sensitive information is authorized on a need-to-know basis.

(g) Develop education and training programs to ensure that individuals are aware of their responsibilities to protect and control classified and sensitive information.

(h) Ensure individuals who prepare and handle classified and sensitive matter are given appropriate training in protection and control procedures consistent with Departmental policies.

(i) Ensure security activities are registered for programs requiring classified information control, in accordance with DOE 5634.1B.

(j) Submit reports of unauthorized disclosures of classified information.

(k) Maintain records of security infractions and determine the disciplinary or corrective action to be taken as a result of infractions.

(l) Establish a self-assessment program for information security.

c. Director of Administration and Management (AD-1), through the Director of Information Resources Management Policy, Plans, and Oversight (AD-24), is responsible for the overall management of the Communications Security (COMSEC), TEMPEST, Protected Distribution System (PDS), Secure Voice, and Unclassified Computer Security (UCS) Programs for the Department, and shall:

(1) Represent the Department as the member to the National Security Telecommunications Information Systems Security Committee (NSTISSC); and

(2) Establish procedures for the dissemination, handling, control, and use of communications security material.

d. Assistant Secretary for Defense Programs (DP-1) shall exercise authorities vested in the Secretary under Executive Order 12356 and in any implementing directives for:

(1) Section 4.2(a) of the Executive order pertaining to creation of defense-related special access programs; and

(2) Section 4.2(b) of the Executive order regarding establishing and maintaining a system for administrative accounting for defense-related special access programs.

e. Assistant Secretary for Nuclear Energy (NE-1) shall exercise authorities vested in the Secretary under Executive Order 12356 and in any implementing directives for:

(1) Section 4.2(a) of the Executive order pertaining to creation of nuclear energy-related special access programs; and

(2) Section 4.2(b) of the Executive order regarding establishing and maintaining a system for administrative accounting for nuclear energy-related special access programs.

f. Deputy Assistant Secretary for Security Evaluations (EH-4) shall:

(1) Direct, manage, and conduct independent inspections, performance tests, and evaluations to assess protection programs and effectiveness of the levels of protection and compliance with security regulations, requirements, and Orders at DOE facilities.

(2) Evaluate the effectiveness of DOE security policies and programs regarding the protection and control of classified information for meeting requirements of applicable statutes and Executive orders.

g. Director of Intelligence (IN-1) shall:

(1) Exercise authorities vested in the Secretary under Executive Order 12356 and in any implementing directives for:

(a) Section 4.2(a) of the Executive order pertaining to creation of special access programs with an intelligence interest;

(b) Section 4.2(b) of the Executive order regarding establishing and maintaining a system for administrative accounting for special access programs with an intelligence interest; and

(c) Authority which has been delegated to the Secretary by the Director of Central Intelligence in furtherance of the provision of sections 3.3(c) and 3.4(e) of the Executive order.

(2) Perform as the Department's point of contact involving activities related to intelligence and counterintelligence, to include oversight of program access to intelligence information provided to or originated within DOE. Coordinate with SA-1 concerning security issues, to include espionage, and the possible or potential compromise of intelligence-related information.

(3) In coordination with SA-1, and consistent with line-management security responsibilities, develop guidelines, instructions, plans, and procedures for the protection of intelligence information consistent with safeguards and security policy.

(4) Through SA-1, coordinate with the Director of Central Intelligence when Sensitive Compartmented Information is unaccounted for or may have been compromised.

h. Director of Security Affairs (SA-1) shall:

(1) Act as the Senior Agency Official responsible for the direction and administration of the DOE Information Security Program.

(2) Exercise authorities vested in the Secretary under Executive Order 12356 and in any implementing directives, except for:

(a) The authority in section 4.2(a) of the Executive order pertaining to creation of special access programs.

(b) The authority in section 4.2(b) of the Executive order regarding establishing and maintaining a system for administrative accounting for special access programs.

(c) Any authority which has been delegated to the Secretary by the Director of Central Intelligence in furtherance of the provision of sections 3.3(c) and 3.4(e) of the Executive order.

(d) The authority to request of the Attorney General an interpretation of the Executive order with respect to any question arising in the course of its administration.

(3) Review and approve policies, standards and requirements for identifying, protecting and controlling classified and sensitive information.

(4) Ensure other Government agencies and foreign governments are informed when their information cannot be accounted for or a compromise may have occurred.

i. Director of Safeguards and Security (SA-10) shall:

(1) Administer and oversee implementation of the Atomic Energy Act of 1954, as amended, for the protection of Restricted Data (RD) and Formerly Restricted Data (FRD).

(2) Administer and oversee implementation of Executive Order 12356 pertaining to special access programs (SAP), personnel, and physical security regarding the protection of National Security Information (NSI).

(3) Provide guidance and assistance in all phases of information security.

(4) Develop, for review and approval by SA-1, policies, standards, and requirements for protecting and controlling classified and sensitive information.

(5) Assist DOE and DOE-contractor activities involving inquiries and damage assessments regarding unaccounted-for classified matter and compromised information.

(6) Designate a Foreign Ownership, Control or Influence (FOCI) Program Manager, who is a DOE employee knowledgeable in FOCI policies and procedures, to manage the DOE FOCI Program.

(7) Designate a Classified Matter Protection and Control (CMPC) Program Manager, who is a DOE employee knowledgeable in control of classified

and sensitive information, including violations of laws, losses, and incidents of security concern, to manage the DOE CMPC Program.

(8) Designate a Classified Computer Program Manager (CCPM), who is a DOE employee knowledgeable in Automated Information Systems (AIS) and AIS Security (AISS), to manage the DOE Classified AISS Program.

(9) Designate a Technical Surveillance Countermeasures (TSCM) Program Manager who is a DOE employee knowledgeable in TSCM operations, to manage the DOE TSCM Program.

(10) Designate an Operations Security (OPSEC) Program Manager, who is a DOE employee knowledgeable in OPSEC, to manage the DOE OPSEC Program.

(11) Notify the Information Security Oversight Office (IS00) of details of unauthorized disclosures.

(12) Assist and advise the Director, Office of Procurement, Assistance and Program Management (through the Office of Policy, (PR-12)) in the development of appropriate Department of Energy Acquisition Regulation (DEAR) prescriptive guidance and clauses to help Heads of Departmental Elements comply with the requirements set forth in paragraph 8b(13); and concur in such developed guidance and clauses.

(13) Administer the Department's subregistry for safeguarding and controlling North Atlantic Treaty-Organization (NATO) classified information. Procedures and requirements for safeguarding and control of NATO classified information are set forth in U.S. Security Authority for NATO Affairs (USSAN) Instruction 1-69 (5100.55, Encl. 2), of 1982.

j. Director of Classification (SA-20) shall:

(1) Administer and oversee the implementation of the Atomic Energy Act of 1954, as amended, with respect to classification policy guidance and the periodic review of RD and FRD for possible declassification.

(2) Exercise authorities vested in the Director of Security Affairs by the Secretary, under Executive Order 12356 and in any implementing directives, pertaining to the classification of information.

k. Deputy Assistant Secretary for Military Applications (DP-20) shall:

(1) Develop policy and requirements, execute approvals and delegations of authority for controlling access to nuclear weapons data in accordance with DOE 5610.2, CONTROL OF WEAPON DATA, of 8-1-80.

(2) For unaccounted-for classified documents or compromised information related to the Joint Atomic Information Exchange Group (JAIEG), coordinate the required reporting to the JAIEG.

l. Managers of DOE Field Offices, in addition to responsibilities at 8b, and, for Headquarters, SA-10, in addition to responsibilities at 8l, shall:

(1) Designate a FOCI Operations Manager, who is a DOE employee knowledgeable in FOCI policies and procedures, to manage the local FOCI Program.

(2) Designate a CMPC Operations Manager, who is a DOE employee knowledgeable in control of classified and sensitive information, including violations of laws, losses, and incidents of security concern, to manage the local program.

(3) Designate a Classified Computer Security Operations Manager, as appropriate, who is a DOE employee knowledgeable in AIS and AIS security, to manage the local classified AIS security program.

(4) Designate a TSCM Operations Manager (TSCMCM), who is a DOE employee cognizant of TSCM operations, to manage the local TSCM program.

(5) Designate an Operations Security (OPSEC) Operations Manager, who is a DOE employee knowledgeable in OPSEC, to manage the local OPSEC program.

(6) Ensure appropriate issuance of infractions to DOE and DOE contractor personnel by:

(a) Designating a DOE Safeguards and Security employee who is knowledgeable in the issuance of infractions.

(b) Ensuring the appointment of DOE contractor personnel knowledgeable in the issuance of infractions.

m. Departmental Information Security Program Managers. Departmental Information Security Program Managers are assigned in SA-10 to manage each element of the Information Security Program identified in paragraph 7. Each Departmental Program Manager, for their assigned area of responsibility, shall:

(1) Represent the DOE on national level committees.

(2) Develop for review by SA-10, and approval by SA-1, policies, standards and procedures.

(3) Provide advice and guidance to Information Security Program Operations Managers in implementing the program.

(4) Establish training for Information Security Program Operations Managers.

(5) Periodically assess the effectiveness of the program.

n. Information Security Program Operations Managers. Operations Managers are assigned by Managers of DOE Field Offices and, for Headquarters, SA-10 to manage elements of the local information security program as described in paragraph 7. Each Operations Manager for their assigned area of responsibility shall:

(1) Ensure the implementation of DOE policy and procedures.

(2) Develop for review by Heads of Field Elements and, for Headquarters, SA-10, and implement local policy and procedures.

(3) Conduct self-assessments to ensure effective implementation.

o. Director of Naval Nuclear Propulsion Program (NE-60) shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by Public Law 98-525 (42 U.S. C. 7158, note)) and to ensure consistency throughout the joint Navy/DOE organization of the Naval Nuclear Propulsion Program, implement and oversee all policy and practices pertaining to Information Security for activities under the Director's cognizance.

p. Procurement Request Originators (the individuals responsible for initiating a requirement on DOE F 4200.33) or such other individual(s) as designated by the cognizant Head of Departmental Element shall bring to the attention of the cognizant contracting officer (1) each procurement requiring the application of this Order, (2) requirement for flowdown of provisions of this Order to any subcontract or subaward, and (3) identification of the paragraphs or other portions of this Order with which the awardee, or, if different, a subawardee, is to comply.

q. Contracting Officers shall, based on advice received from the procurement request originator or other designated individual, apply applicable provisions of this Order to awards falling within its scope. For awards, other than management and operating contracts, this shall be by incorporation or reference using explicit language in a contractual action.

9. SECURITY ORGANIZATION.

a. Within each organization a clearly identifiable chain of responsibility for information security shall exist between the organization's top management and its working levels.

b. To ensure the operation of an effective Information Security Program, the following program guidelines shall be established:

(1) The organization's management shall ensure that adequate personnel and other resources are made available to implement and maintain the information security program.

(2) Security management shall be staffed with knowledgeable individuals.

(3) Individuals responsible for managing or implementing information security programs shall be provided adequate time and resources to accomplish assigned functions satisfactorily in accordance with Orders.

10. CLASSIFIED PROGRAM MANAGEMENT.

a. Heads of Departmental Elements responsible for programs requiring classified matter protection and control shall ensure that classified matter security procedures are established and are approved by the cognizant security office before the start of such programs.

b. New programs shall be reviewed by an authorized classifier to determine if the activities being performed are classified or sensitive and therefore require control. Once a formal, documented determination has been made that classified or sensitive information is involved, the identity and classification of the information shall be forwarded to the appropriate security office.

c. Management shall be involved in, and supportive of, all aspects of information security. This active involvement with, and support for security activities and programs will be demonstrated by the manager or a designated representative regularly visiting and inspecting information security operations to ensure that operations are in compliance with existing standards and policies.

d. Management shall ensure that information security is included in protection program planning documents.

11. ACCESS TO CLASSIFIED AND SENSITIVE INFORMATION.

a. Access to classified information shall be granted only to persons who possess the appropriate security clearance and need-to-know. Supervisors or other responsible officials who are knowledgeable of the classified information and the responsibilities of the individual may make the determination of need-to-know. It is the responsibility of the individual disseminating classified information to ensure that the recipient of the information has the appropriate security clearance and need-to-know. Access to classified information shall be based on DOE access requirements, as specified in DOE 5631.2C, PERSONNEL SECURITY PROGRAM, of 9-15-92.

b. Before a facility is eligible for custody (possession) of classified matter, a DOE facility clearance must be granted in accordance with DOE , 5634.16

c. Access to sensitive information shall be granted only to persons who possess the appropriate need-to-know. It is the responsibility of the individual disseminating sensitive information to ensure that the recipient of the information has the appropriate need-to-know.

d. Individuals are responsible for protecting all classified and sensitive information to which they have access or custody. In furtherance of this requirement, the individual shall comply with the provisions set forth in this and other DOE safeguards and security related Orders.

12. STORAGE. Classified matter, when not in actual use and under the control of an appropriately cleared person, shall be stored and protected in accordance with DOE 5632.5, PHYSICAL PROTECTION OF CLASSIFIED MATTER.

13. UNACCOUNTED-FOR/COMPROMISED MATTER OR COMPROMISES OF INFORMATION.

a. Unaccounted-For Matter. This paragraph pertains to those situations where classified matter has been or may have been lost, missing, or otherwise unaccounted-for.

(1) Discovery. Any person who determines that classified matter has been or may have been lost, is missing, or is otherwise unaccounted-for shall take immediate action to preclude any further or potential compromises and report this information to the custodian or security officer. The measures listed below apply to custodians who determine or learn that classified matter is unaccounted-for.

(2) Initial Search. Upon determining or learning that classified matter may be unaccounted-for, a search of the immediate area where the matter was stored, handled, or processed shall be conducted. When applicable, the accountability records shall be audited for evidence of destruction, transmission, or other disposition.

(a) If the matter is found or otherwise accounted-for with no indication of compromise, no further actions need to be taken.

(b) If Secret or Confidential matter is unaccounted-for, the cognizant safeguards and security organization or officer shall be notified within 24 hours from initial indications of the unaccounted-for status.

(c) If Sigma 1 or Sigma 2 Weapon Data matter is unaccounted-for, the Office of Safeguards and Security (SA-1O), the appropriate Secretarial Officer, and the Office of Military Applications

(DP-20), through the cognizant safeguards and security organization or officer shall be notified within 24 hours.

(d) If Top Secret matter, classified matter of another agency, or classified matter of a foreign government is unaccounted-for, SA-10 and the appropriate Secretarial Officer, through the cognizant safeguards and security organization or officer, shall be notified within 24 hours. Documents related to the Joint Atomic Information Exchange Group (JAIEG) shall also be reported to DP-20 who will ensure appropriate reporting to JAIEG.

(3) Detailed Search. Unaccounted-for matter that cannot be reconciled after the initial search and audit of records shall require a more detailed search of the area where the matter may have been stored, processed, and handled. Additionally, custodians of document control stations providing immediate adjacent support, as well as one level above and one level below the holder must be queried. The facility's security organization shall initiate a detailed search in an attempt to ascertain whether or not a transmittal, receipt, or destruction may have been administratively mishandled. The detailed search and query process shall be completed within 48 hours. If the matter is found, or otherwise accounted-for, the search process will be discontinued; however, the facility security office shall review the surrounding circumstances and procedures for possible corrective action.

(4) Preliminary Inquiry. The purpose of a preliminary inquiry is to establish whether a compromise of classified information or a violation of law has occurred. Preliminary inquiries shall be conducted as expeditiously as possible and shall not be used as a means of holding in abeyance a decision to initiate a full-scale inquiry.

(a) When all efforts fail to reconcile unaccounted-for matter, the facility security office shall initiate a preliminary inquiry to document and ensure all basic areas of consideration have been satisfied. As a minimum the preliminary inquiry shall:

1 Include an interview with the last known custodian and require that individual, and any other personnel who may have pertinent information, prepare signed memoranda on the protection and control of the matter or the circumstances under which the matter became unaccounted-for.

2 Include a review by an authorized classifier of the classification assigned to the matter at the time it was determined unaccounted-for. If another copy of the unaccounted-for matter exists, arrangements shall be made to review the current classification and hold the copy for possible future reviews.

3 Ensure the conduct of a physical search of the office of the last known holder and other offices where the matter may logically be found. A part of any search shall include a review of the custodian's records, the central files, and the local central document control office (including downgrade and declassification notices, destruction certificates, classified document receipts, letters or transmittal, and incoming and outgoing mail logs).

4 Determine the reason why the matter is unaccounted-for and recommend action to prevent recurrence.

5 Assess the potential for compromise and determine if additional investigation is required.

6 Provide adequate information to be used to complete the Department of Justice eleven point criteria if deemed necessary.

(b) The preliminary inquiry shall be completed and a written report, DOE F 5635.11, "Reporting Unaccounted For Documents," or a form similar in content, with supporting statements/documentation, shall be forwarded to the cognizant Departmental Element safeguards and security organization or officer. A classification review of the form shall be performed by an authorized derivative classifier. An example of DOE F 5635.11 is shown as Attachment 3. The cognizant Departmental Element safeguards and security organization or officer shall notify SA-10 and the responsible Secretarial Officer in accordance with DOE 5000.3A, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, of 5-30-90.

(c) The preliminary inquiry shall review the circumstances, procedures, and activities surrounding the incident, and provide for-corrective action to preclude recurrence.

(5) Records. (See paragraph 13e for records retention). For accountability purposes, classified matter may be removed from accountability records, if any, and maintained in a separate record of unaccounted-for matter when:

(a) All inquiries have been completed; and

(b) Corrective actions have been implemented (commitments to implement shall not constitute implementation).

b. Compromised Information. If the compromise or potential compromise is a result of an unaccounted-for document, the procedures in paragraph 13a will satisfy parallel requirements identified below.

(1) Discovery. Any person who discovers that classified information has been, or may have been, compromised shall take immediate action to secure the classified information and report the discovery to the facility security office.

(2) Preliminary Inquiry.

(a) Upon notification of a possible compromise, the facility security office shall initiate a preliminary inquiry to document the circumstances surrounding the possible compromise and notify the cognizant safeguards and security organization or officer. The DOE safeguards and security organization or officer shall advise SA-10 of the initiation of a preliminary inquiry. As a minimum the inquiry shall include:

1 Signed statements by individuals who may have knowledge regarding the circumstances surrounding the possible compromise.

2 A review by an authorized classifier of the classification assigned to the information at the time of the possible compromise. When matter is involved, a copy of the matter shall be held for possible future reviews.

3 A signed memorandum from the document custodian, if documents were involved, regarding the protection and control of the document at the time of the possible compromise.

4 A determination of how the possible compromise occurred and recommended actions to prevent recurrence.

(b) Preliminary inquiry shall be completed and a written report with-supporting statements/documentation shall be forwarded to SA-10 and the responsible Secretarial Officer through the cognizant safeguards and security organization or officer. When the possible compromise involves information or matter from another Government agency or foreign government, SA-1 shall ensure the other agency or government is informed of the results of the inquiry.

(c) When a preliminary inquiry establishes credible information that a violation of law may have occurred, notification to SA-10 and the Secretarial Officer is required and the reporting requirements identified in DOE 5000.3A must be followed. Upon completion of the Department of Justice (DOJ) Eleven-point Criteria, the Federal Bureau of Investigation (FBI) shall be notified. These criteria have been established to assist DOE in conducting preliminary inquiries prior to passage to DOJ. A positive response must be provided to all eleven points for DOJ to initiate a formal

investigation. All documentation and appropriate information must be provided to support the affirmative responses.

1 Could the date and identity of the article or articles disclosing the classified information be provided?

2 Could specific statements in the article which are considered classified be identified? Was the data properly classified?

3 Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.

4 Did the data come from a specific document and, if so, what is the origin of the document and the name of an individual(s) responsible for the security of the classified data disclosed?

5 Could the extent of official dissemination of the data be determined?

6 Has it been determined that the data has not been officially released in the past?

7 Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?

8 Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?

9 Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.

10 Has it been determined that declassification had not been accomplished prior to the publication or release of the data?

11 Will the disclosure of the classified data have an adverse impact on the national defense?

(3) Detailed Review.

(a) Upon notification from the facility security office that the preliminary inquiry has been completed, the cognizant DOE safeguards and security organization or officer shall initiate a detailed review to:

1 Establish the party or parties responsible for the compromise of the classified information.

2 Review protection and control and other security procedures in place.

3 Ensure corrective actions are taken to preclude recurrence of conditions or activities that allowed or contributed to the compromise of classified information.

(b) A report of the detailed review shall be prepared. This report shall contain the following information and be transmitted to the cognizant Secretarial Officer:

1 A complete description of the circumstances which led to the discovery of the compromised information;

2 A complete description of the nature of information involved (e.g.,, document, oral disclosure) to include date, subject, classification level and category;

3 The estimated likelihood and extent of compromise with full justification for the conclusions reached, supported by factual information;

4 The individual(s) to whom any infractions have been assigned and the disciplinary actions taken, if any;

5 Cause for the compromise (e.g., procedural or human failure); and

6 The measures taken or contemplated to correct deficiencies or prevent recurrence. If contemplated, provide estimated completion dates. Include plan of action to ensure that measures are taken.

(c) When classified information of another Government agency or foreign government are involved, SA-1 will ensure they are informed of the results of the detailed review for their use.

(d) When a detailed review establishes credible information that a violation of law may have occurred, the matter shall be referred to the FBI, which has the responsibility for investigating alleged or suspected violations of Federal law. Notification to SA-10 and the responsible Secretarial Officer is required and the reporting requirements identified in DOE 5000.3A must be followed.

(e) If the results of the detailed review indicate that a compromise has occurred or may have occurred and the cognizant Secretarial Officer decides it can reasonably be expected to result in a compromise, the Secretarial Officer will appoint a DOE employee to conduct a damage assessment.

c. Damage Assessments. Damage assessments are required by 32 CFR, Chapter XX, Part 2000, "National Security Information," Section 2001.47 "Loss or Possible Compromise." The purpose of the damage assessment is to assess potential damage to the national security in terms of programmatic impact. Therefore the damage assessment will be most useful to the Secretarial Officer in determining future courses of action within the program. The damage assessment is also useful to security personnel in assessing possible countermeasure and cover actions to limit the assessed damage.

When the inquiry into the loss of classified information or unaccounted-for classified matter discloses evidence that information may have been compromised and a compromise of the information can reasonably be expected to cause damage to the national security, a damage assessment shall be conducted. Compromises may occur through espionage, unauthorized disclosures to press or other members of the public, loss of classified information, unaccounted-for classified matters, or through various other circumstances. Both the circumstances of the loss and the sensitivity of the information must be considered in determining when a damage assessment is required.

(1) Conduct of Damage Assessment. The Secretarial Officer with programmatic responsibility for the compromised information will appoint a DOE individual responsible for conducting the damage assessment and appoint an assessment team consisting of an authorized classifier and appropriate technical experts (e.g., weapons design, nuclear policy, material production communications, intelligence, etc.) to assist in the assessment of the value of the compromised information to foreign governments or hostile organizations.

(2) Procedures. The following procedures shall be followed for all DOE damage assessments.

(a) The originator of the compromised information shall provide the cognizant Departmental Element safeguards and security organization or officer with a copy of the compromised information (including a copy of the matter, if appropriate) and rationale/justification for the assigned classification with reference to appropriate classification guides.

(b) The originator shall immediately notify all holders of the matter that it has been compromised.

(c) A review of previous damage assessments performed within DOE, on file at SA-10, will be conducted by the team performing the damage assessment to determine if the same or similar information has been previously compromised, and the results of the damage assessment.

(d) A draft assessment will be prepared by the team performing the damage assessment and coordinated with the originator.

(e) The damage assessment will then be approved by the Secretarial Officer with programmatic oversight of the information and submitted to SA-1.

(f) The assessment team will provide any additional assessment effort and supporting documentation needed by SA-10 to complete any required DOE action.

(3) Damage assessments shall be in writing, and as a minimum, contain the following:

(a) Identification of the source, date, and circumstances of the compromise.

(b) Classification of the specific information lost.

(c) A description of the specific information lost.

(d) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

(e) An assessment of the possible advantage to foreign powers resulting from the compromise.

(f) An assessment of whether the classification of the information involved should be continued without change; the specific information or parts thereof, that shall be modified to minimize or nullify the effects of the reported compromise and the classification retained; and downgrading, declassification, or upgrading is warranted and, if so, confirmation of prompt notification to holders of any change.

(g) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(h) An assessment of other appropriate corrective, administration, disciplinary, or legal actions.

(4) Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with the DOE General Counsel (GC-1).

(5) Compromise of outside agencies' classified information shall be reported to the originating agency by SA-1. The report to the originating agency must include all data pertinent to the compromise to assist in their conduct of a damage assessment.

(6) Damage assessments may be completed for a group of unaccounted-for classified matter discovered during inventory whenever grouping is a logical method of meeting this requirement. A logical grouping includes a situation when multiple matters requiring a damage assessment are related to a programmatic area and would result in similar damage to the national security or advantage to foreign powers.

(7) Compromise Involving Another Government Agency's Information:

(a) The other agency has the inherent responsibility to conduct the damage assessment on their information that was lost/compromised.

(b) Whenever a compromise involves the classified information of DOE and another agency, and if more than one damage assessment is performed, the Departmental Element responsible for the DOE damage assessment shall provide, through SA-1, the findings to the other agency.

(c) When a joint assessment is to be made, SA-1 will coordinate the assignment of responsibility between DOE and the other agency.

(d) Whenever a compromise of DOE classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals in the employ of international organizations, SA-1 shall ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained.

(e) Whenever a compromise of Sensitive Compartmented Information (SCI) has occurred, IN-1 shall consult with the designated representative of the Director of Central Intelligence (DCI) and other appropriate officials with responsibility for the information involved.

d. Notification to Information Security Oversight Office (ISOO). On receiving written confirmation from a Departmental Element of an unauthorized disclosure of, or access to, NSI by a DOE employee, DOE contractor, or consultant, SA-10 shall notify the IS00 of the details of such a disclosure. Such notification shall be given immediately when the

disclosure results from systematic problems. Otherwise, semi annual reports of unauthorized disclosures shall be made.

e. Records Retention. Records of all actions pertaining to unac counted-for/compromised matter or compromises of information must be maintained by the facility and the cognizant Departmental Element safeguards and security organization or officer. In accordance with DOE 1324.2A, RECORDS DISPOSITION, of 9-13-88, records shall be destroyed 5 years after the close of all associated actions. These records will not be sent to Federal Records Centers.

14. SECURITY INFRACTIONS. An infraction is an act or omission involving failure to comply with Departmental safeguards and security Orders.

a. Examples of Infractions. The following actions represent instances wherein a "Report of Security Infraction" may be issued. The list is not all-inclusive. If it is determined that any of these actions were intentional or caused by gross negligence, such action may constitute a "violation," resulting in criminal prosecution or other administrative actions.

(1) Classified matter exposed and unattended or unsecured at the close of business or whenever a room is unattended.

(2) Improper storage of classified matter.

(3) Failure to safeguard or account for classified matter resulting in the compromise or potential compromise of the documents.

(4) Removal of classified matter from a security area without proper authorization.

(5) Failure to obtain classification guidance thereby causing a compromise or possible compromise of classified information.

(6) Changing of a document's classification status without proper authorization.

(7) Failure to properly safeguard combinations of repositories containing classified matter.

(8) Destruction of classified matter in other than the prescribed manner.

(9) Improper transmission of classified matter.

(10) Discussion of classified information over unsecured telephone systems.

(11) Failure to escort uncleared persons in security areas.

(12) Permitting an unauthorized person to hear, obtain visual access to, or otherwise obtain classified information.

(13) Failure to safeguard a computer access password.

(14) A computer work-station containing classified information or connected to a classified host computer unattended.

b. Report of Security Infraction. DOE F 5630.13, "Report of Security Infraction" or a form similar in content shall be used to document security infractions and a copy of the report kept in the employee's official DOE personnel security file. An example of DOE F 5630.13 is shown as Attachment 4. With each occurrence security practices or procedures shall be reviewed and revised if necessary to preclude recurrence.

c. Records of Security Infractions. The responsible safeguards and security organization or officer reporting the security infraction and the cognizant Departmental Element shall maintain records of each infraction, which shall include all pertinent facts associated with the infraction.

(1) For DOE employees, the disciplinary or corrective action shall be determined by the Heads of Departmental Elements in coordination with the Office of Personnel. Any disciplinary or adverse action in connection with a DOE employee shall be taken in accordance with DOE personnel policies and procedures (see DOE 3750.1, WORK FORCE DISCIPLINE, of 3-23-83).

(2) For contractors and other persons under their jurisdiction, the disciplinary or corrective action shall be determined by appropriate management officials in accordance with the contractors' personnel policies and procedures.

(3) For military personnel and employees of other Government agencies assigned to DOE or DOE contractors, DOE or its contractors shall take corrective action and submit a report of infractions to the military organization or Government agency to which the employee is permanently assigned for whatever disciplinary action that the cognizant agency or organization deems necessary.

15. EMERGENCY PROCEDURES. Organizations shall develop procedures for safeguarding classified matter during emergencies. The procedures shall be as simple and practical as possible and should be adaptable to meet most emergencies that may arise.

16. SELF-ASSESSMENTS. Self assessments will be addressed by the overall self-assessment program. Organizations shall establish a self-assessment program for the purpose of evaluating all information security procedures applicable to the facility's operations. Organizations shall review their security programs

on a continuing basis and shall also conduct a formal self-assessment to occur between inspections conducted in accordance with the schedules required by DOE 5634.1B. Self-assessments shall consist of an examination of the facility's operations in light of its security plan and the requirements contained in DOE Orders. Deficiencies identified as a result of self-assessments shall be corrected promptly. A record of the self-assessment shall be maintained until the next DOE inspection is conducted in accordance with DOE 5634.1B.

BY ORDER OF THE SECRETARY OF ENERGY:

DOLORES L. ROZZI
Director of Administration
and Management

REFERENCES

1. Atomic Energy Act of 1954, as amended:

   a. Chapter 12, "Control of Information," section 141-146, inclusive, which sets forth the principles for the control of Restricted Data.

   b. Chapter 14, 'General Authority," section 161, "General provisions," which sets forth the authority necessary to perform the function of the Department and the Nuclear Regulatory Commission.

   c. Chapter 18, "Enforcement," sections 221-233, which sets forth the authority necessary to protect Restricted Data and to safeguard property and establish criminal penalties for violation of provisions of the Atomic Energy Act.

2. Department of Energy Acquisition Regulation (DEAR) 904.70 - Foreign Ownership, Control or Influence Over Contractors - This clause sets forth the policies and procedures for FOCI over contractors.

3. DEAR 952.204 "Clauses Related to Administrative Matters" sets forth the security clauses to be used in DOE contracts. They are:

   a. DEAR 952.204-2 "Security Requirements" is required in contracts under Section 31 (research assistance) or 41 (ownership and operation of production facilities) of the Atomic Energy Act of 1954, as amended, and in other contracts and subcontracts, the performance of which involves or is likely to involve classified information.

   b. DEAR 952.204-70 "Classification" is to be used in all contracts that involve classified information.

   c. DEAR 952.204-73 "Foreign Ownership, Control, or Influence Over Contractors (Representation)" requires contracting officers to insert the provision of this part in all solicitations for contracts subject to the provisions of DEAR 904.70.

   d. DEAR 952.204-74 "Foreign Ownership, Control or Influence Over Contractors" requires contracting officers to insert the stated contract clause in this part in new contracts and contract modifications to existing contracts subject to DEAR 904.70.

4. Title 18, United States Code (U.S.C.), Section 798, “Disclosure of Classified Information,” of 1988, which provides for definitions, enforcement, and penalties for crimes and criminal procedures relating to the disclosure of classified information.

5. Executive Order 12356, “National Security Information,” of 4-6-82, which provides requirements for safeguarding National Security Information, and “Information Security Oversight Office Directive No. 1,” of 6-25-82, which assists in implementing Executive Order 12356.

6. Title 10 Code of Federal Regulations (CFR), Part 1016, “Safeguarding of Restricted Data,” which establishes policy and requirements for the protection of Restricted Data.

7. Title 32 CFR, Chapter XX, Part 2000, “National Security Information,” which establishes policy and requirements for incidents of loss or possible compromise of classified matter.

8. National Security Decision Directive Number 84 (NSDD 84), of 3-11-83, which sets the requirements for safeguarding National Security Information against unlawful disclosures.

9. DOE 1324.2A, RECORDS DISPOSITION, of 9-13-88, which sets the requirements regarding the retention and disposition requirements for Government records.

10. DOE 1324.5A, RECORDS MANAGEMENT PROGRAM, of 4-30-92, which provides the scope, objectives, and authority for the records management program of DOE.

11. DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, of 5-18-92, which establishes policy for safeguarding DOE AIS systems and, in particular, DOE unclassified sensitive information.

12. DOE 3750.1, WORK FORCE DISCIPLINE, of 3-23-83, which provides guidance and procedures for maintaining work force discipline in the Department of Energy.

13. DOE 5000.3A, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, of 5-30-90, which establishes a system for reporting of operations information related to DOE-owned or operated facilities and processing of that information to provide for appropriate corrective action.

14. DOE 5300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST), of 5-18-92, which establishes the DOE telecommunications program for emissions security.

15. DOE 5300.3C, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY (COMSEC), of 5-18-92, which establishes policy, responsibilities, and guidance concerning the communication security (COMSEC) aspects of telecommunications services of the DOE, and implements the national telecommunications protection policy.

16. DOE 5300.4C, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEM, of 5-18-92, which establishes policy for the DOE concerning protected distribution systems used for the transmission of unencrypted classified or unclassified sensitive information related to national security.

17. DOE 5610.2, CONTROL OF WEAPON DATA, of 8-1-80, which establishes procedures for controlling weapon data.

18. DOE 5630.8A, SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION, of 7-31-90, which promulgates the official definition of naval nuclear propulsion information, outlines disclosure policies and general safeguarding requirements for such matter, and clarifies the requirements for disposal of matter containing naval nuclear propulsion information.

19. DOE 5630.11, SAFEGUARDS AND SECURITY PROGRAM, of 1-22-88, which establishes policy and responsibility for the DOE Safeguards and Security Program.

20. DOE 5631.2C, PERSONNEL SECURITY PROGRAM, of 9-15-92, which establishes policy, responsibilities, and authorities for implementing the DOE Personnel Security Program.

21. DOE 5639.3, VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 9-15-92, which sets forth Departmental procedures to ensure timely and effective investigation and other followup action relating to violations of Federal laws and to certain losses involving security interests.

22. DOE 5632.1B, PROTECTION PROGRAM OPERATIONS, of 9-8-92, which prescribes policies, responsibilities, and authorities for the physical protection of security interests and establishes minimum physical protection requirements and standards for such interests.

23. DOE 5632.5, PHYSICAL PROTECTION OF CLASSIFIED MATTER, of 2-3-88, which establishes DOE policy and objectives for the physical protection of classified matter and establishes baseline physical protection requirements and standards for those interests.

24. DOE 5634.1B, FACILITY APPROVAL, SECURITY SURVEYS, AND NUCLEAR MATERIALS SURVEYS, of 9-15-92, which establishes Departmental requirements for conducting periodic security surveys of classified facilities under the Department’s jurisdiction. The Department shall ensure that all facilities eligible to receive, process, reproduce, store, transmit, or handle classified matter,

including special nuclear materials, have been granted facility approval prior to permitting access to such matter or material.

25. DOE 5635.1A, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION, of 2-12-88, which provides guidance relative to the safeguarding and control of classified documents and information.

26. DOE 5635.4, PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION, of 2-03-88, which establishes DOE policy and procedures for the protection of Unclassified Controlled Nuclear Information (UCNI).

27. DOE 5637.1A, CLASSIFIED COMPUTER SECURITY PROGRAM, of 9-15-92, which establishes uniform requirements, policies, responsibilities, and procedures for the development and implementation of a Department of Energy Classified Computer Security Program to ensure the security of classified information in Automated Data Processing systems.

28. DOE 5639.5, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 8-3-92, which establishes the Department's Technical Surveillance Countermeasures (TSCM) Program.

29. DOE 5639.7, OPERATIONS SECURITY, of 4-30-92, which establishes the DOE Operations Security Program.

30. DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, of 12-31-91, which provides specific responsibilities, standards, and procedures for managing the DOE classification system.

31. DOE 5650.3A, IDENTIFICATION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION, of 6-8-92, which establishes policy and procedures for identifying Unclassified Controlled Nuclear Information (UCNI) and for reviewing and marking documents and material containing UCNI.

32. DOE 5670.1A, MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE, of 1-15-92, which sets the guidelines for managing and assigning responsibilities for the Department's foreign intelligence activities.

33. DOE 5639.8, SECURITY OF FOREIGN INTELLIGENCE INFORMATION AND SENSITIVE COMPARTMENTED INFORMATION FACILITIES, of 9-15-92, which establishes responsibilities and authorities for the protection of Foreign Intelligence Information and Sensitive Compartmented Information Facilities.

DEFINITIONS

1. ACCESS. Refers to the following:

   a. The knowledge, use, or possession of classified or other sensitive information required by an individual to perform his/her official duties that is provided to the individual on a need-to-know basis.

   b. The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures which are in force do not prevent gaining knowledge of the classified information.

2. ACCESS AUTHORIZATION OR SECURITY CLEARANCE. An administrative determination that an individual is eligible for access to classified information or special nuclear material on a "need-to-know" basis. Clearances granted by the Department are designated Q, L, Top Secret, or Secret.

3. ASSESSMENT.

   a. An evaluation of the effectiveness of an activity/operation or a determination of the extent of compliance with required procedures and practices.

   b. An appraisal of the credibility, reliability, pertinency, accuracy or usefulness of information.

4. AUTHORIZED PERSON. A person who has a need-to-know for classified information in the performance of official duties and who has been granted the required personal clearance.

5. AUTOMATED INFORMATION SYSTEMS SECURITY (AISS) PROGRAM. See Classified Computer Security (COMPUSEC) Program.

6. CLASSIFICATION.

   a. Original Classification. The initial determination that information requires protection as National Security Information (NSI) under the provisions of Executive Order 12356. This includes the specification of a classification level and the classification duration.

b. Derivative Classification.

(1) Restricted Data (RD) or Formerly Restricted Data (FRD). A determination in accordance with approved classification guidance or source documents that a document or material contains RD or FRD.

(2) National Security Information (NSI). A determination in accordance with approved classification guidance, source documents, or other instructions from an original classifier that a document or material contains NSI.

7. CLASSIFICATION CATEGORY. One of three kinds of classified information; that is, Restricted Data, Formerly Restricted Data, or National Security Information.

8. CLASSIFICATION LEVEL. A designation assigned to specific elements of information based on the potential damage to national security if disclosed to unauthorized persons. The three classification levels in descending order of potential damage are Top Secret, Secret, and Confidential.

9. CLASSIFIED COMPUTER SECURITY PROGRAM. All of the technological safeguards and managerial procedures established and applied to ADP facilities and ADP systems (including computer hardware, software, and data) in order to ensure the protection of classified information.

10. CLASSIFIED DOCUMENT. Any document containing classified information.

11. CLASSIFIED INFORMATION. Certain information requiring protection against unauthorized disclosure in the interests of national defense and security or foreign relations of the United States pursuant to Federal statute or Executive order. The term includes Restricted Data, Formerly Restricted Data, and National Security Information. The potential damage to the national security of each is denoted by the classification levels Top Secret, Secret, or Confidential. (See CLASSIFICATION LEVEL and CLASSIFICATION CATEGORY.)

12. CLASSIFIED MATERIAL.

a. Chemical compounds, metals, fabricated or processed items, machinery, electronic equipment, and equipment or any combination thereof that has been assigned a classification level and classification category.

b. Any combination of documents, products, substances, or material that has been assigned a classification either individually or as a group.

13. COMMUNICATIONS SECURITY (COMSEC). Measures and controls that deny information derived from telecommunications to unauthorized persons and ensure the authenticity of such telecommunications. NOTE: Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

14. COMPLIANCE. Meeting DOE safeguards and security requirements set forth in Orders and-other guidance.

15. COMPROMISE. Disclosure of classified information to unauthorized persons.

16. COMPUTER SECURITY (COMPUSEC). The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system.

17. CONFIDENTIAL. A classification level that is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

18. CONTRACTING OFFICER. A Government official who, in accordance with departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his/her authority.

19. CONTRACTOR. An entity or person who contracts directly or indirectly to supply goods or services to the DOE. NOTE: This includes subcontractors of any tier, consultants, agents, grantees, and cooperative agreement participants.

20. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) Department of Defense marking for TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA revealing the theory-of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems, limited life components, and totally contained quantities of fissionable, fusionable, and high-explosive materials by type. Among these excluded items are the components which military personnel, including contractor personnel, set, maintain, operate, test, or replace.

21. DAMAGE ASSESSMENT. An analysis of the impact on national security of disclosure of classified information to an unauthorized person(s).

22. RECLASSIFICATION.

a. Information. A determination by appropriate authority in accordance with approved classification policy that information is no longer classified; or

b. Documents or Material. A determination by appropriate authority in accordance with approved classification guidance that a classified document or material no longer contains classified information; and

c. The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

23. DECLASSIFICATION AUTHORITY. The authority to determine that (a) information or (b) documents, or material may be declassified and to effect such declassification.

24. DOCUMENT. Any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electric recordings in any form.

25. EMANATIONS SECURITY. Refers to security measures designed to deny unauthorized persons access to important information which might be derived from intercepting and analyzing compromising emanations from other than crypto equipment and telecommunications systems.

26. EMISSION SECURITY. Protective measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

27. EVALUATION. Determination of the effectiveness of a safeguards and security system or program element relative to approved standards.

28. FACILITY. An educational institution, manufacturing plant, laboratory, office building: or complex of buildings located on the same site that is operated and protected as one unit by the Department or its contractor(s).

29. FOREIGN GOVERNMENT INFORMATION.

a. Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

b. Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any elements thereof, requiring that the information, the arrangement, or both are to be held in confidence.

30. FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI). Foreign ownership, control, or influence exists when a DOE contractor performing classified work, or having access to significant quantities of special nuclear material, has an institutional or personal relationship with a foreign interests. A contractor is considered to be under foreign ownership, control, or influence when the degree of interest as defined above is such that a reasonable basis exists for concluding that compromise of classified information or a significant quantity of special nuclear material, as defined in 10 CFR 710, may result.

31. FORMERLY RESTRICTED DATA (FRD). Classified information jointly determined by the DOE or its predecessors and the DOD to be related primarily to the military utilization of atomic weapons, and removed by the DOE from the Restricted Data category pursuant to Section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

32. FOR OFFICIAL USE ONLY. Information that has not been given a security classification pursuant to the criteria of an Executive order, but which may be withheld from public disclosure under the criteria of the Freedom of Information Act, Title 5, U.S.C., Section 552. (NOTE: EQUIVALENT TO THE DOE "OUO").

33. INCIDENT OF SECURITY CONCERN. Events which, at the time of occurrence, cannot be determined to be an actual violation of law, but which are of such significant concern to the DOE Safeguards and Security Program as to warrant immediate preliminary investigation, review or inquiry and subsequent reporting. NOTE: Examples include: drug use and distribution, alcohol abuse, criminal racketeering or other organized criminal activity, the loss or theft of firearms, the discovery or possession of contraband articles in security areas, and unauthorized attempts to access classified databases.

34. INFORMATION. Facts, data, or knowledge itself, rather than the medium of its conveyance. (Documents and material are deemed to convey or contain information and are not considered to be information per se.)

35. INFORMATION SECURITY (INFOSEC). This term refers to the result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by Executive order or statute.

36. INFORMATION SECURITY OVERSIGHT OFFICE (ISOO). An organization within the General Services Administration responsible for implementing and monitoring Government implementation of Executive Order 12356 "National Security Information." The National Security Council provides overall policy direction for this program.

37. INFRACTION. An act or omission involving failure to comply with DOE safeguards and security order directives.

38. INSPECTION. The process of gathering information to determine the effectiveness with which protection programs are implemented.

39. MATTER. Any combination of documents, computer media, information, or material.

40. NATIONAL SECURITY. The national defense and foreign relations of the United States.

41. NATIONAL SECURITY INFORMATION (NSI). Any information that has been determined pursuant to Executive Order 12356 or any predecessor order to require protection against unauthorized disclosure and that is so designated. The levels TOP SECRET, SECRET and CONFIDENTIAL are used to designate such information.

42. NAVAL NUCLEAR PROPULSION INFORMATION (NNPI). Information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities. NOTE: Information concerning equipment, components, or technology that is applicable to both naval nuclear and conventional propulsion plants is not considered to be NNPI when used in reference to conventional applications only, provided no association with naval nuclear propulsion can be directly identified from the information in question. In cases where an association with naval nuclear propulsion can be directly identified from the information in question, designation of the information as NNPI is mandatory. Some unclassified NNPI is also Unclassified Controlled Nuclear Information.

43. NEED-TO-KNOW. A determination by a person having responsibility for classified information or material that a proposed recipient's access to such classified information or matter is necessary in the performance of official or contractual duties of employment.

44. OFFICIAL USE ONLY (OUO).

a. Information that has not been given a security classification pursuant to the criteria of an Executive order, but which may be withheld from public disclosure under the criteria of the Freedom of Information Act, Title 5, U. S. C., Section 552. (NOTE: EQUIVALENT TO THE DOD USE OF "FOUO").

b. A security classification marking during the period 7-18-49 through 10-22-51 l

45. OPERATIONS SECURITY (OPSEC). A program designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive DOE activities or information and to prevent the unauthorized disclosure of such information.

46. PROGRAM SECRETARIAL OFFICER (PSO). A senior outlay program official that includes the Assistant Secretaries for Conservation and Renewable Energy, Defense Programs, Fossil Energy, Nuclear Energy, Environmental Restoration and Waste Management, and the Directors of Energy Research and Civilian Radioactive Waste Management. A lead PSO is the PSO assigned line management responsibility and accountability for Headquarters and field operations and to which one or more multi-program Field Offices report directly.

47. RESTRICTED DATA (RD) . All data concerning: design, manufacture or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

48. SAFEGUARDS AND SECURITY ACTIVITY. Any work performed under contract, subcontract, or other agreement which involves access to classified information, nuclear material, or DOE property of significant monetary value by DOE, a DOE contractor, or any other activity under DOE jurisdiction. Also included is the verification of the capabilities of approved Federal locations.

49. SECRET. The classification level applied to classified matter of which the unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

50. SECRETARIAL OFFICERS. Those individuals identified as Program or Staff Secretarial Officers.

51. SECURITY. An integrated system of activities, systems, programs, facilities, and policies for the protection of Restricted Data and other classified information or matter, nuclear materials, nuclear weapons and nuclear weapon components, and/or Departmental and Departmental contractor facilities, property, and equipment.

52. SENSITIVE INFORMATION. Information, the disclosure of which could reasonably be expected to adversely affect national or DOE security interests. This includes both classified and unclassified information and matter (e.g., Export Controlled Information, Naval Nuclear Propulsion Information, Unclassified Controlled Nuclear Information, Official Use Only Information, and certain unclassified information, or matter) as identified in program Critical and Sensitive Information Lists.

53. SENSITIVE COMPARTMENTED INFORMATION. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the , Director of Central Intelligence.

54. SPECIAL ACCESS PROGRAM (SAP) . Any program established under Executive Order 12356 or the Atomic Energy Act of 1954, as amended, that imposes additional controls governing access to classified information involved with such programs beyond those required by normal management and safeguarding practices. These programs may include, but are not limited to, access approval, adjudication or investigative requirements, special designation of officials authorized to determine a need-to-know, or special lists of persons determined to have a need-to-know. Within DOE, a SAP is one category of Special Access Required programs.

55. STAFF SECRETARIAL OFFICERS. Includes: the General Counsel; Assistant Secretaries for Congressional and Intergovernmental Affairs, Environment, Safety and Health, Domestic and International Energy Policy; the Inspector General; Chief Financial Officer; Administrators, Economic Regulatory Administration and Energy Information Administration; Directors of Administration and Management; Emergency Planning and Operations, Intelligence, Minority Economic Impact, Nuclear Safety, Procurement, Assistance and Project Management, Small and Disadvantaged Business Utilization, Security Affairs, Hearings and Appeals, Arms Control and Nonproliferation, Contractor Employee Protection, Departmental Representative to the Defense Nuclear Facilities Safety Board, Public Affairs, Special Projects, and Scheduling and Logistics; and the Chairman, Board of Contract Appeals.

56. TECHNICAL SECURITY. Includes technical surveillance countermeasures (TSCM), communications security (COMSEC), and the prevention or suppression of compromising emissions and emanations.

57. TECHNICAL SURVEILLANCE. The covert installation of devices or equipment to visually or audibly monitor activities within a target area to acquire information by technical means.

58. TECHNICAL SURVEILLANCE COUNTERMEASURE (TSCM). Systematic and effective measures for the detection and nullification of technical surveillance penetrations, technical surveillance hazards, and physical security weaknesses.

59. TEMPEST. Short name ref erring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

60. TOP SECRET (TS). The Cl assification level applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the nat ional security; the highest classification level.

61. UNAUTHORIZED DISCLOSURE. A communication or physical transfer of classified information to an unauthorized recipient.

62. UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI). Certain unclassified Government information whose unauthorized dissemination is prohibited under Section 148 of the Atomic Energy Act of 1954, as amended and DOE 5650.3A, IDENTIFICATION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION.

63. VIOLATION. Alleged, suspected, or actual criminal breach of Federal laws.

64. VULNERABILITY. An exploitable capability or an exploitable security weakness or deficiency at a facility of national security interest. Exploitable capabilities or weaknesses are those inherent in the design (or layout) of the facility and its protection, or those existing because of the failure to meet (or maintain) prescribed safeguards and security standards when evaluated against Department of Energy requirements for defined threats.

65. WEAPON DATA. Restricted Data or Formerly Restricted Data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices.

REPORTING UNACCOUNTED-FOR DOCUMENTS

DOE F 5635.11
(1-84)
(Previously DP-M178)

U.S. DEPARTMENT OF ENERGY

REPORTING UNACCOUNTED FOR DOCUMENTS

The following information is furnished to the Director of Safeguards and Security, in accordance with HQ Appendix 2105 and in follow-up to the oral report made by Charles H. Chan (Name) to Richard Cook, Director, OSS/SR (Name of Security Representative) on February 15, 1987 (Date)

J. J. Johnson (Signature of Office Director, or Division Head) February 17, 1987 (Date)

(If possible avoid including information that would necessitate classification of this form)

1. DOCUMENT IDENTIFICATION

(a) Document number (T/S identification, weapon data report, research and development report, etc.)
None

(b) Copy number 3 of 6 copies, series A
Number of pages 7

(c) Date of document
December 6, 1986

(d) Classification
Top Secret ☐ Secret ☒ Confidential ☐

(e) [illegible] Information
[illegible] Restricted Data ☐ Restricted Data ☒
[illegible] Defense Information ☐

(f) Title or subject
Tritium Production Projections [illegible]ents 1990-1995

(g) Originator
Lion Chemical Corporati[illegible]

(h) Addressee
P.O. Box 711
Lincoln, TN 66666

(i) Type of document (size, color, memora[illegible] original, carbon copy, photostat, etc.)
Booklet, 8½X11 inches, blue cover, stapled on left margin, cover memo signed by Chan.

EXAMPLE

2. OFFICE ACCOUNTABILITY

(a) Date document entered office accountability
January 5, 1987

(b) Personnel in office who have had access to existing copies as well as unaccounted for copy (or copies)
Martin W. Chan, Supervisor (Cy 3)
Charles Smith, Accountability (Cy 1)
Larry P. Jones, Analyst (Cy 2)

(c) Personnel outside office who have had access to existing copies as well as unaccounted for copy (or copies)
Linda B. Leonard, Chemist, (Cy 5)
Terri Parker, Accountability (Cy 6)
L. Harrison, Dalton, V.P. Binder Chem. (Cy

3. UNACCOUNTABILITY

(a) Time and date document was first determined unaccounted for
February 14, 1987

(b) Full statement regarding unaccountability. Use blank portion on reverse side or attach extra sheet to include the following

(1) Reason why document is believed to be misfiled or definitive statement of destruction without record, *OR*
(2) Indication or allegation that the document(s) have been either stolen, concealed, misappropriated, or lost under circumstances indicating violation of Federal statue, *AND*
(3) Whether or not document is considered to be of great importance to the DOE program and reasons therefor, *AND*
(4) If appropriate, statement of improper possession by unauthorized persons

REPORTING UNACCOUNTED-FOR DOCUMENTS

4. OFFICE ACTION

(a) Person responsible for this security infraction. Martin W. Chan, Supervisor, Production Division

(b) Corrective action taken with person responsible for this security infraction.

This is Mr. Chan's first security infraction and counseling was conducted in accordance with DOE 5635.1A. Mr. Chan was made aware that subsequent infractions will result in more stringent measures.

(c) Corrective action taken to prevent recurrence of similar incident in the future.

All office personnel have been brieifed and advised that the proper return of documents to files and strict accountability must be maintained. Procedures outlined in DOE 5635.1A must be followed.

(d) Result of search to account for document(s), including statement that all files in division or office have been checked.

A detailed search of the three repositories under Mr. Chan's control has been initiated and is continuing. A final report will be provided not later than February 22, 1987.

(e) Attach signed statement by person responsible for security infraction. Statements by all other persons involved in the unaccountability of the document(s)

This space is to be used for completion of item 3 or other necessary. Extra sheets shall be attached in order to complete this report.

The unaccounted-for document is believed to be misfiled. On Feburary 13, 1987, at 0800 hours, the document was removed from the Division files and the sign-out sheet was initialled by Mr. Chan. The document was returned at 1400 hours and the sign-out form appropriately initialled showing its return. Two other office members that could have had access to the repository were on travel and could not have had access to the document when the unaccountability occured. Mr. Chan is positive that he returned the document but has not been able to locate it as of February 17, 1987. It is not believed that the document has been compromised but rather mis-placed/filed. Mr. Chan is continuing an inventory of the repositories and will advise the Document Control Facility and OSS Division of the final results by February 20, 1987. The document is considered to be a critial sensitive document and every effort is being taken to locate the document. A copy of the document has been forwarded to the Office of Classification for a classification determination.

REPORT OF SECURITY INFRACTION

DOE F 5630.13
(1-84)
(Previously DP-M 184)

U.S. DEPARTMENT OF ENERGY

REPORT OF SECURITY INFRACTION

Part I.–NOTIFICATION OF INFRACTION

To Be completed by Office of Safeguards and Security and sent to Office concerned.

1. Office in which infraction occurred: Office of the Controller

2. Date: 4-10-87

3. Nature of infraction:

Unsecured Security Container #123

4. Details of infraction:

While on routine security patrol, Safe #123, located in Room 4A-111, Forrestal Building, was found in an open condition by Officer Smith, Jones Security Service, at 7:30 p.m., April 10, 1987. Attempts to contact the responsible individuals as listed on the SF 700, "Security Container Information", met with negative results. In addition, SF 702, "Security Container Check Sheet", has no entries for opening or closing the safe on 4-10-87. The safe was secured at 8:00 p.m., by the guard supervisor, Captain Smith.

EXAMPLE

Part II.–RE... ...CERNED

To be completed by the Office in whic... ...d returned to Office of Safeguards and Security within 3 days after ... ...above.

1. Name and title of person acknowled... ...onsibility:

Martha A. Williams, Administrative Assistant, Office of the Controller

2. Highest classification of material involved: Confidential ☐ Secret ☒ Top Secret ☐

3. Was "Restricted Data" involved? Yes ☐ No ☒

4. Reason or cause for infraction: This safe is used to temporarily store documents by Ms. Williams in her day-to-day activities. On 4-10-87, she received several documents that were intended for other staff members who at the time were out to lunch. Ms. williams opened the safe and placed the documents inside with the intention of giving them to the members on their return; however, the members did not return and the safe was not secured nor was the check sheet annotated.

5. Corrective action taken (*see reverse side for suggested disciplinary action*):

Ms. Williams has been interviewed by me regarding the serious nature of this matter and will take extra precautions in the future to prevent recurrence of incidents such as this. In addition,a system for checking this safe has been instituted. This will include someone verifying the safe is locked at the close of each working day.

6. Signature of Office Director: James J. Dallas

7. Date: 4-12-87

* U.S. G.P.O.:1992-342-169:80012