DOE 5639.3
9-15-92

THIS PAGE MUST BE KEPT WITH DOE 5639.3, VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS.

DOE 5639.3, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, HAS REVISED DOE 5631.5 TO REFLECT ORGANIZATIONAL TITLE, ROUTING SYMBOL, AND OTHER EDITORIAL REVISIONS REQUIRED BY SEN-6. NO SUBSTANTIVE CHANGES HAVE BEEN MADE. DUE TO THE NUMBER OF PAGES AFFECTED BY THE REVISIONS, THE ORDER HAS BEEN ISSUED AS A REVISION. THE NUMBER OF THE ORDER HAS BEEN CHANGED TO 5639.3 TO REFLECT ITS PROPER DESIGNATION WITHIN THE INFORMATION SECURITY SERIES OF ORDERS.

U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5639.3

9-15-92

SUBJECT: VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS

1. PURPOSE. To set forth Department of Energy (DOE) procedures to assure timely and effective action relating to violations of criminal laws, losses, and incidents of security concern to DOE.

2. CANCELLATION. DOE 5631.5, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 2-12-88.

3. SCOPE. The provisions of this Order apply to all Departmental Elements and contractors performing work for the Department as provided by law and/or contract and as implemented by the appropriate contracting officer.

4. REFERENCES. See Attachment 1.

5. DEFINITIONS. See Attachment 2.

6. POLICY. It is the policy of DOE to protect special nuclear materials, classified matter, and property whose theft, destruction or damage would impact DOE activities and operations by maintaining security programs and procedures which deter, detect, and ensure the prompt reporting of actual or suspected criminal violations, losses of classified matter or special nuclear material and incidents of security concern to DOE.

7. RESPONSIBILITIES AND AUTHORITIES.

   a. Secretarial Officers shall:

      (1) Establish directives and implementing procedures to ensure the provisions of this Order are met at facilities or activities for which they are responsible.

      (2) Obtain the written approval of the Director of Safeguards and Security (SA-1O) for exceptions to the provisions of this Order.

      (3) Ensure a damage assessment is initiated by a DOE element or Federal agencies, as appropriate, in accodance with the requirements of Title 32, Code of Federal Regulations (CFR), Chapter XX, Part 2000, "National Security Information," Section 2001.47, "Loss or Possible Compromise,"

DISTRIBUTION:

All Departmental Elements

INITIATED BY:

Office of Security Affairs

when a violation, loss, or incident of security concern can reasonably be expected to cause damage to the national security.

(4) Ensure that field elements complete the necessary actions to resolve violations, losses, and incidents of security concern, including actions to prevent recurrence.

b. Director of Security Affairs (SA-1), through the Director of Safeguards and Security (SA-10):

(1) Develops policies and procedures for the reporting of violations, losses, and incidents of security concern.

(2) Prepares reports regarding violations, losses, and incidents of security concern for submission to the Secretary, other Government agencies, and the Congress.

(3) Serves as the primary point of liaison with the Federal Bureau of Investigation (FBI), Headquarters, the local FBI, and law enforcement and security agencies, including Federal counterintelligence organizations, for the operational aspects of violations, losses, and incidents of security concern.

(4) Serves as the primary point of liaison with the Office of Inspector General (IG-1), Headquarters, for matters involving violations, losses, and incidents of security concern.

(5) Provides consultation and assistance, as required, to field elements in the conduct of preliminary inquiries to develop information as to the probability of a violation, loss, or incident of security concern. Also, provides consultation and assistance in the conduct of subsequent investigations.

(6) Administers the program for the conduct of preliminary internal inquiries of unlawful disclosures of classified information to meet the requirements of National Security Decision Directive 84, "Safeguarding National Security Information," of 3-11-83, and DOE guidelines, "Guide for Conducting Preliminary Internal Inquiries," as set forth in Chapter II.

(7) At DOE Headquarters:

(a) Reports violations, losses, and incidents of security concern to the Inspector General, the FBI, and other responsible Headquarters Elements, as appropriate.

(b) Conducts preliminary inquiries and takes appropriate followup actions in response to violations, losses, and incidents of security concern, including actions to prevent recurrence.

(c) Provides for the preparation of bomb data programs or nuclear threat incident reports for those incidents occurring within the jurisdiction of Headquarters.

(8) Reviews and, as appropriate, grants exceptions to the provisions of this Order.

c. Director of Intelligence (IN-1) through the Director of Threat Assessment (IN-30).

(1) Provides timely assessments of actual or potential threats to DOE interests.

(2) Acquires, evaluates, processes, analyzes, and disseminates strategic, tactical, and other forms of information necessary in characterizing the range of malevolent acts and adversaries posing actual/potential threats. I

(3) Develops procedures and conducts a program for the assessment of nuclear security incidents.

(4) Conducts liaison with the Federal Bureau of Investigation (FBI) and other appropriate Federal agencies on the threat assessment matters.

(5) Consults with the Central Intelligence Agency (CIA) whenever a compromise of Sensitive Compartmented Information (SCI) has occurred, consistent with page I-2, paragraph 1b(2).

d. Director of Emergency Planning and Operations (OE-1) through the Headquarters Emergency Operations Center (EOC).

(1) Serves as the focal point for the reporting of violations, losses, and incidents of security concern which warrant immediate Headquarters notification.

(2) Notifies SA-10 and other responsible Headquarters Elements, as appropriate.

e. Heads of Field Elements.

(1) Through the contracting officer, assure that contractors establish procedures to report all violations, losses, and incidents of security concern promptly to DOE in accordance

with the provisions of this Order and DOE 5000.3A, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION.

(2) Conduct preliminary inquiries of violations, losses, and incidents of security concern to DOE.

(3) Provide timely progress reports to SA-10 of all followup actions taken and to the Offices of Military Application (DP-20), Weapons and Materials Planning (DP-27), and Naval Reactors (NE-60), when DOE nuclear weapons, components, or special nuclear material associated with the weapons program, are involved.

(4) Maintain a close and continuing liaison with the offices of the FBI and other law enforcement and counterintelligence agencies within their geographic jurisdiction.

(5) Maintain a close and continuing liaison with the cognizant office of the Inspector General.

(6) Prepare and submit reports of violations, losses, and incidents of significant security concern for such occurrences within their jurisdiction, in accordance with DOE 5000.3A.

(7) Prepare and submit bomb incidents reports in accordance with the FBI "Bomb Data Incident Form."

(8) Request review and approval by the cognizant PSO and SA-10 for exceptions to the provisions of this Order.

f. Inspector General (IG-1).

(1) Develops policies and procedures for the reporting of fraud, waste, and abuse as defined in Title 42, United States Code (U.S.C.) 7138, which fall under the purview of the Inspector General (IG-1).

(2) Conducts inquiries and investigations of fraud, waste, and abuse matters involving DOE or DOE contractors in coordination with the FBI and other law enforcement agencies as stipulated by policy set forth in DOE 2320.1C, COOPERATION WITH THE OFFICE OF INSPECTOR GENERAL, and other interagency agreements and law.

(3) Maintains liaison with the SA-10 and other responsible Headquarters Elements, as appropriate, on matters affecting the security of nuclear materials and classified activities including possible criminal activity by DOE cleared personnel.

g. General Counsel (GC-1) advises on preliminary inquiries into possible violations of criminal law, losses, and incidents of security concern to DOE, to ensure conformity of actions with applicable laws.

h. Director, 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 this DOE Order for activities under the Director's cognizance.

BY ORDER OF THE SECRETARY OF ENERGY:

DOLORES L. ROZZI
Director of Administration
and Human Resource Management

REFERENCES

1. The Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011 et seq.; section 148 et seq., relating to the prohibition against the dissemination of unclassified information; and section 7138 et seq., relating to fraud, waste, and abuse matters.

2. DOE 2320.1C, COOPERATION WITH THE OFFICE OF INSPECTOR GENERAL, of 5-18-92, which establishes policy for cooperation with the Office of the Inspector General.

3. "Guide for Conducting Preliminary Internal Investigations," which provides a uniform system for conducting investigations (see Chapter II).

4. The Internal Security Act of 1950, as amended, 50 U.S.C. 47a, concerning illegal introduction, manufacture, acquisition, or export of special nuclear materials or atomic weapons, or conspiracies relating thereto; section 781 regarding control of subversives; section 784 regarding employment of members of communist organizations; and section 797 on security regulations and orders and the penalty for violation.

5. National Security Decision Directive 84, "Safeguarding National Security Information," of 3-11-83, which establishes responsibilities for ensuring that nondisclosure agreements are obtained.

6. The Privacy Act of 1974, which establishes requirements for protection of personal information.

7. DOE 5000.3A, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, of 5-30-90, which establishes a DOE system for identification, categorization, notification, analysis, reporting, followup and closeout of occurrences.

8. Title 10 CFR 1017, Identification and Protection of Unclassified Controlled Nuclear Information, which establishes overall policies and procedures for the identification and protection of UCNI.

9. Title 18 U.S.C., relating to:

   a. Espionage or information control (sections 792-98);

   b. Sabotage (sections 2151-56);

   c. Treason and subversive activity (sections 2381-85);

   d. Actual or threatened use of explosives against persons or property (sections 841-48);

   e. Embezzlement and theft (sections 641 and 6619) ;

f. Extortion and threats (sections 876-78) ;

g. Riots (section 2101);

h. Acts of malicious mischief (sections 1362-63); and

i. Theft and destruction of Government property and civil disorders (section 231).

10. Title 32 CFR Chapter XX, Part 2000, "National Security Information," Section 2001.47, "Loss or Possible Compromise," which requires the conduct of damage assessments in instances involving the loss or possible compromise of classified information.

DEFINITIONS

1. CLASSIFIED MATTER. Classified information, documents or material.

2. CONTRACTOR(S). Those individuals and/or organizations under direct contract to the DOE and includes subcontractors, individuals, or organizations under contract to a contractor.

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

4. 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).

5. FORMERLY RESTRICTED DATA (FRD). Classified information jointly determined by the DOE or its predecessors and the Department of Defense 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.

6. INCIDENTS OF SECURITY CONCERN. Those incidents as defined on page 3, paragraph 16c(1) through (9) and paragraph 16g, of this Attachment, which, at the time of occurrence, cannot be determined to be an actual criminal violation of law, but which are of such significant concern to the DOE Safeguards and Security program as to warrant immediate preliminary investigation and subsequent reporting, as specified in this Order. Examples include, but are not limited to, the following: 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.

7. INTERNAL SECURITY REPORT. An account, complying with the Privacy Act of 1974, concerning known or suspected potential threats to DOE and DOE contractor facilities within the geographic jurisdiction of a field element. A report may result from information received through contacts with Federal, State, and local law enforcement or counterintelligence officials within the vicinity of the respective field organization and contractor facility.

8. LOSS. Any situation involving:

   a. A loss of classified matter, documents or material, or special nuclear material outside a security area even though there are no circumstances indicating a violation of criminal law.

b. A loss of classified matter, documents or material, or special nuclear material within a security area, if there is no immediate explanation to account for the loss, even though there are no circumstances indicating a violation of criminal law.

9. MATERIAL. Chemical substances, fabricated items, assemblies, machinery or equipment.

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

11. 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.

12. PRELIMINARY INQUIRY. A review of the circumstances surrounding a suspected or alleged criminal violation or loss involving the national security to develop all pertinent information and to determine whether a criminal violation has occurred.

13. RESTRICTED DATA. 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 Restricted Data category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.

14. SECURITY INCIDENT REPORT. A report in the form of a memorandum, teletype, telefax, facsimile, or other electronic means of an actual or suspected violation, loss, or other incident of security concern.

15. SPECIAL NUCLEAR MATERIAL (SNM). Plutonium, uranium-233, or uranium enriched in the isotope 235, and any other material which, pursuant to the provisions of section 51 of the Atomic Energy Act of 1954, as amended, has been determined to be special nuclear material, but does not include source material; or it also includes any material artificially enriched by any of the foregoing, but does not include source material.

16. VIOLATION. Alleged or suspected criminal violations of, or relating to:

a. The Atomic Energy Act of 1954, as amended:

(1) Title 42 U.S. C. 2011 et seq.;

(2) Title 42 U.S. C. 148 et seq., relating to the prohibition against the dissemination of certain unclassified information; and

(3) Title 42 U.S. C. 7138 et seq., relating to fraud, waste, and abuse matters.

b. The Internal Security Act of 1950, as amended, 50 U.S.C. 781 and 784 et seq.

c. Title 18 U.S.C. relating to:

(1) Espionage or information control (sections 792-98);

(2) Sabotage (sections 2151-56);

(3) Treason and subversive activity (sections 2381-85);

(4) Actual or threatened use of explosives against persons or property (sections 841-48);

(5) Embezzlement and theft (sections 641 and 6619);

(6) Extortion and threats (sections 876-78);

(7) Riots (section 2101);

(8) Acts of malicious mischief (sections 1361-63); and

(9) Theft and destruction of Government property and civil disorders (section 231).

d. Title 10 CFR Part 1017, "Identification and Protection of Unclassified Controlled Nuclear Information."

e. Other criminal statutes having a relationship to the security of DOE project activities, facilities, or classified information.

f. Instances when classified documents (or classified configurations) or source and special nuclear material are missing under circumstances that indicate a violation of criminal law.

g. Nuclear security incidents, defined as any situation involving the threatened, attempted, or actual theft, loss, or unauthorized use, possession, or sale of: source or special nuclear material radioactive byproducts; nuclear explosive devices (either separately or in combination with explosives); and radioactive dispersal devices.

h. Bomb incidents, defined as any situation involving the threatened, attempted, or actual use of conventional explosives including the malevolent use of flammable, corrosive, or toxic materials.

TABLE OF CONTENTS

CHAPTER I

SCOPE OF POLICY, PROCEDURES, AND REPORTING REQUIREMENTS

1. SCOPE OF POLICY.

a. DOE and DOE Contractor Employees.

(1) Representatives shall not conduct any investigations of criminal violations as defined in Attachment 2, paragraph 16. An exception to this is when DOE investigators are deputized agents of the State or local law enforcement agencies. Such deputized agents, however, shall consult with the FBI when investigating criminal violations involving DOE and DOE contractor activities, operations, or personnel.

(2) Employees with knowledge of, or information indicating possible fraud, waste, abuse, or other forms of wrong doing in the Department's programs or operations shall inform IG-1 immediately upon obtaining such knowledge or information as defined in DOE 2320.1C.

(3) DOE representatives may conduct preliminary internal investigations of unlawful disclosures of classified information consistent with paragraph 7, "Responsibilities and Authorities."

(4) IG-1 is responsible for conducting preliminary inquiries and investigations of fraud, waste, or abuse by DOE and DOE contractor employees, consistent with paragraph 7.

(5) Loss or compromise of documents and material, and violations of criminal laws relating to matters of security concern to DOE and DOE contractors shall be reported promptly to SA-10 and to the the FBI.

b. Other Federal Agencies.

(1) Federal Bureau of Investigation (FBI).

(a) The FBI of the Department of Justice has the responsibility for investigating alleged or suspected violations of criminal laws or statutes involving the national security.

(b) FBI special agents will be given all appropriate and lawful assistance, including technical advisory assistance, as needed. They shall be admitted to areas and afforded access to Restricted Data or other classified information as may be necessary in the performance of their duties. Such special agents shall be provided escort, as necessary, for safety reasons or to facilitate investigations progress.

(c) FBI special agents shall be advised at the time of access of the classification and the category of the information, whether seen or heard (i.e., Restricted Data, Formerly Restricted Data, or National Security Information). Appropriate document and data classification and marking information should be made available to the FBI special agents through local liaison channels.

(d) The availability of photo identification badges and advance notification arrangements shall be determined by agreement between the DOE and FBI organizations involved. This authority does not extend to Sensitive Compartmented Information, which requires special access approval.

(2) Central Intelligence Agency (CIA). The designated representatives of the Director, Central Intelligence Agency, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of Sensitive Compartmented Information (SCI), has occurred, consistent with the policy set forth in 32 CFR Chapter XX, Part 2000 "National Security Information," Section 2001.47, "Loss or Possible Compromise."

2. REPORTING PROCEDURES The method and sequence of the reporting of violations, losses, and incidents of security concern will depend upon the situation as well as the immediacy of action which may be required to mitigate the situation. Reports of violations, losses, and incidents of significant security concern to DOE which require immediate oral reporting shall be made in accordance with DOE 5000.3A. Appropriate security incident reports in the form of a memorandum, teletype, telefax, facsimile, or other electronic means shall be submitted to the appropriate authorities as soon as the required information becomes available.

CHAPTER II

GUIDE FOR CONDUCTING PRELIMINARY INTERNAL INQUIRIES

1. PURPOSE.

   a. This chapter establishes a uniform system within the DOE for conducting preliminary internal inquiries of unlawful disclosures of classified information consistent with the policy set forth in National Security Decision Directive 84, "Safeguarding National Security Information."

   b. The purpose of a preliminary internal inquiry is to establish whether a compromise of classified information has occurred and, if so, to make a damage assessment and a determination whether a violation of law is in evidence; and also recommend actions, if appropriate, to mitigate or lessen the damage to the national security. 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 investigation.

2. ORGANIZATIONAL RESPONSIBILITIES.

   a. Safeguards and Security Representatives. Representatives of safeguards and security offices may conduct preliminary internal inquiries as required to establish the circumstances surrounding a suspected or alleged criminal violation or loss involving a national security interest. The authority to conduct such inquiries remains with the Head of the Field Element and, in the case of Headquarters, with SA-10.

   b. Federal Bureau of Investigation. When a preliminary internal inquiry establishes credible information that a national security violation of law may have occurred, the matter shall be referred to the Federal Bureau of Investigation, which has the responsibility for investigating alleged or suspected violations of Federal laws.

   c. Office of the Inspector General. When a preliminary internal inquiry establishes credible information that a criminal violation which does not involve a-national security interest has occurred, the Office of the Inspector General shall be notified for information and/or action of the possible violation.

3. PROCEDURES. For the purpose of this chapter, a generic term, "Violation of Security," shall refer to unlawful disclosures of classified information, compromises of classified information, and lost documents.

   a. Appointment of Inquiry Official. All efforts shall be made to appoint a DOE inquiry official (with previous inquiry experience) who is familiar with policies and procedures concerning security of classified information.

b. Assignment of Responsibility for the Violation of Security. Whenever possible, the inquiry shall fix responsibility upon an individual rather than upon a position or office. When individual responsibility cannot be established, and the facts show that a responsible official allowed conditions to exist which led to a violation of security, responsibility shall be fixed upon such responsible official.

c. Preliminary Inquiry Report. The preliminary inquiry report should contain the following information:

(1) A complete description of the circumstances which led to the discovery of the violation of security;

(2) A complete description of the nature of information involved (document or 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 (i.e., conclusions that a lost document had been destroyed) must be supported by factual information.

(4) The individual upon whom the responsibility has been fixed and the disciplinary action taken, if any.

(5) Cause for the compromise (i.e., procedural or human failure).

(6) The measures taken or contemplated to correct deficiencies or prevent recurrence. If contemplated, provide estimated completion date. Include plan of action to ensure that measures were taken.

(7) Assessment of the damage to national security.

(8) A statement of whether further investigation is warranted.

d. Reporting Intervals.

(1) In all cases of a reported and confirmed violation of security, the field elements shall immediately report such violations to SA-10. Oral reports shall be confirmed in writing within 24 hours.

(2) A preliminary internal inquiry shall be instituted within 48 hours from the initial report of the violation of security to SA-10 and cognizant Secretarial Officer.

(3) A preliminary inquiry report shall be submitted to SA-10 and cognizant Secretarial Officer within 20 working days, and status reports shall be provided every 10 days until closure of the case (extension of time may be granted by SA-10).