United States Department of the Interior
Office of the Secretary

Interior Business Center

Interior Business Center
Human Resources Operations Division
Personnel Security Branch
Security Clearance Briefing Material

Extracts of the Espionage & Sabotage Acts and other Federal Criminal Statutes

18 U.S. Code

§ 793. Gathering, transmitting or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense,

(1) Through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or

(2) Having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer— Shall be fined under this title or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

§ 794. Gathering or delivering defense information to aid foreign government

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or, if there is no jury, the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning

systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.
(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

§ 795. Photographing and sketching defense installations

(a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

(b) Whoever violates this section shall be fined under this title or imprisoned not more than one year, or both.

§ 796. Use of aircraft for photographing defense installations

Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment, in violation of section 795 of this title, shall be fined under this title or imprisoned not more than one year, or both.

§ 797. Publication and sale of photographs of defense installations

On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined under this title or imprisoned not more than one year, or both.

§ 798. Disclosure of classified information

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) Concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) Concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) Concerning the communication intelligence activities of the United States or any foreign government; or

(4) Obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—
Shall be fined under this title or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—
The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

§ 2155. Destruction of national-defense materials, national-defense premises, or national-defense utilities

(a) Whoever, with intent to injure, interfere with, or obstruct the national defense of the United States, willfully injures, destroys, contaminates or infects, or attempts to so injure, destroy,

contaminate or infect any national-defense material, national-defense premises, or national-defense utilities, shall be fined under this title or imprisoned not more than 20 years, or both, and, if death results to any person, shall be imprisoned for any term of years or for life.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

§ 2156. Production of defective national-defense material, national-defense premises, or national-defense utilities

(a) Whoever, with intent to injure, interfere with, or obstruct the national defense of the United States, willfully makes, constructs, or attempts to make or construct in a defective manner, any national-defense material, national-defense premises or national-defense utilities, or any tool, implement, machine, utensil, or receptacle used or employed in making, producing, manufacturing, or repairing any such national-defense material, national-defense premises or national-defense utilities, shall be fined under this title or imprisoned not more than ten years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

§ 371. Conspiracy to commit offense or to defraud United States

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both. If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

50 U.S.Code

§ 797. Penalty for violation of security regulations and orders

(a) Misdemeanor violation of defense property security regulations

(1) Misdemeanor: Whoever willfully violates any defense property security regulation shall be fined under title 18 or imprisoned not more than one year, or both.

(2) Defense property security regulation described: For purposes of paragraph (1), a defense property security regulation is a property security regulation that, pursuant to lawful authority—

(a) Shall be or has been promulgated or approved by the Secretary of Defense (or by a military commander designated by the Secretary of Defense or by a military officer, or a civilian officer or employee of the Department of Defense, holding a senior Department of Defense director

position designated by the Secretary of Defense) for the protection or security of Department of Defense property; or
(b) Shall be or has been promulgated or approved by the Administrator of the National Aeronautics and Space Administration for the protection or security of NASA property.

(3) Property security regulation described**:** For purposes of paragraph (2), a property security regulation, with respect to any property, is a regulation—
(a) Relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse, or other unsatisfactory conditions on such property, or the ingress thereto or egress or removal of persons there from; or

(b) Otherwise providing for safeguarding such property against destruction, loss, or injury by accident or by enemy action, sabotage, or other subversive actions.

(4) Definitions in this subsection:

a) Department of Defense property**:** The term "Department of Defense property" means covered property subject to the jurisdiction, administration, or in the custody of the Department of Defense, any Department or agency of which that Department consists, or any officer or employee of that Department or agency.

(b) NASA property**:** The term "NASA property" means covered property subject to the jurisdiction, administration, or in the custody of the National Aeronautics and Space Administration or any officer or employee thereof.

(c) Covered property**:** The term "covered property" means aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places.

(d) Regulation as including order**:** The term "regulation" includes an order.

(b) Posting**:** Any regulation or order covered by subsection (a) of this section shall be posted in conspicuous and appropriate places.

32 CFR Parts 2001 and 2003 Classified National Security Information

Effective Date: June 25, 2010.

Subpart E--Safeguarding

Sec. 2001.40 General.

(a) Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification.

(b) Except for foreign government information, agency heads or their designee(s) may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. When alternative measures are used for other than temporary, unique situations, the alternative measures shall be documented and provided to the Director of ISOO. Upon request, the description shall be provided to any other agency with which classified information or secure facilities are shared. In all cases, the alternative measures shall provide protection sufficient to reasonably deter and

detect loss or unauthorized disclosure. Risk management factors considered will include sensitivity, value, and crucial nature of the information; analysis of known and anticipated threats; vulnerability; and countermeasure benefits versus cost.
(C) North Atlantic Treaty Organization (NATO) classified information shall be safeguarded in compliance with U.S. Security Authority for NATO Instruction (USSAN) 1-07. Other foreign government information shall be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation (hereinafter, obligation). When the information is to be safeguarded pursuant to an existing obligation, the additional requirements at Sec. 2001.54 may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment. Negotiations on new obligations or amendments to existing obligations shall strive to bring provisions for safeguarding foreign government information into accord with standards for safeguarding U.S. information as described in this Directive.

(d) Need-to-know determinations. (1) Agency heads, through their designees, shall identify organizational missions and personnel requiring access to classified information to perform or assist in authorized governmental functions. These mission and personnel requirements are determined by the functions of an agency or the roles and responsibilities of personnel in the course of their official duties. Personnel determinations shall be consistent with section 4.1(a) of the Order.

(2) In instances where the provisions of section 4.1(a) of the Order are met, but there is a countervailing need to restrict the information, disagreements that cannot be resolved shall be referred by agency heads or designees to either the Director of ISOO or, with respect to the Intelligence Community, the Director of National Intelligence, as appropriate. Disagreements concerning information protected under section 4.3 of the Order shall instead be referred to the appropriate official named in section 4.3 of the Order.

Sec. 2001.41 Responsibilities of holders.

Authorized persons who have access to classified information are responsible for:

(a) Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person;

(b) Meeting safeguarding requirements prescribed by the agency head; and

(c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

Sec. 2001.42 Standards for security equipment.

(a) Storage. The Administrator of the General Services Administration (GSA) shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications, qualified product lists or databases, and supply schedules for security equipment designed to provide secure storage for classified information. Whenever new secure storage equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of the GSA, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

(b) Destruction. Effective January 1, 2011, only equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) may be utilized to destroy classified information using any method covered by an EPL. However, equipment approved for use prior

to January 1, 2011, and not found on an EPL, may be utilized for the destruction of classified information until December 31, 2016. Unless NSA determines otherwise, whenever an EPL is revised, equipment removed from an EPL may be utilized for the destruction of classified information up to six years from the date of its removal from an EPL. In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly, the unit must be taken out of service for the destruction in accordance with this section. The Administrator of the GSA shall, to the maximum extent possible, coordinate supply schedules and otherwise seek to make equipment on an EPL available through the Federal Supply System.

Sec. 2001.43 Storage.

(a) General. Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government-controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board.

(b) Requirements for physical protection--(1) Top Secret. Top Secret information shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with Sec. 2001.53. In addition, supplemental controls are required as follows:

(i) For GSA-approved containers, one of the following supplemental controls:

(A) Inspection of the container every two hours by an employee cleared at least to the Secret level;

(B) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation. Acceptability of Intrusion Detection Equipment (IDE): All IDE must be in accordance with standards approved by ISOO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head; or
(C) Security-In-Depth coverage of the area in which the container is located, provided the container is equipped with a lock meeting Federal Specification FF-L-2740.

(ii) For open storage areas covered by Security-In-Depth, an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(iii) For open storage areas not covered by Security-In-Depth, personnel responding to the alarm shall arrive within five minutes of the alarm annunciation.

(2) Secret. Secret information shall be stored in the same manner as Top Secret information or, until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock. Security-In-Depth is required in areas in which a non-GSA-approved container or open storage area is located. Except for storage in a GSA-approved container or a vault built to FED STD 832, one of the following supplemental controls is required:

(i) Inspection of the container or open storage area every four hours by an employee cleared at least to the Secret level; or

(ii) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

(3) Confidential. Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

(c) Combinations. Use and maintenance of dial-type locks and other changeable combination locks.

(1) Equipment in service. Combinations to dial-type locks shall be changed only by persons authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:

(i) Whenever such equipment is placed into use;

(ii) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or

(iii) Whenever a combination has been subject to possible unauthorized disclosure.

(2) Equipment out of service. When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the combination lock should be reset to a standard combination of 50-25-50 for built-in combination locks or 10-20-30 for combination padlocks.

(d) Key operated locks. When special circumstances exist, an agency head may approve the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be included in implementing regulations required under section 5.4(d)(2) of the Order.

(e) Repairs. The neutralization and repair of GSA-approved security containers and vault doors will be in accordance with FED STD 809.

Sec. 2001.44 Reciprocity of use and inspection of facilities.

(a) Once a facility is authorized, approved, certified, or accredited for classified use, then all agencies desiring to conduct classified work in the designated space(s) at the same security level shall accept the authorization, approval, certification, or accreditation without change, enhancements, or upgrades provided that no waiver, exception, or deviation has been issued or approved. In the event that a waiver exception, or deviation was granted in the original accreditation of the designated space(s), an agency seeking to utilize the designated facility space may require that a risk mitigation strategy be implemented or agreed upon prior to using the space(s).

(b) Subsequent security inspections or reviews for authorization, approval, certification, or accreditation purposes shall normally be conducted no more frequently than annually unless otherwise required due to a change in the designated facility space(s) or due to a change in the use or ownership of the facility space(s). This does not imply a formal one-year inspection or review requirement or establish any other formal period for inspections or review.

Sec. 2001.45 Information controls.

(a) General. Agency heads shall establish a system of control measures which assure that access to classified information is provided to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures which may include records of internal distribution, access, generation, inventory, reproduction, and disposition of classified information shall be required

when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons.

(1) Combinations. Combinations to locks used to secure vaults, open storage areas, and security containers that are approved for the safeguarding of classified information shall be protected in the same manner as the highest level of classified information that the vault, open storage area, or security container is used to protect.

(2) Computer and information system passwords. Passwords shall be protected in the same manner as the highest level of classified information that the computer or system is certified and accredited to process. Passwords shall be changed on a frequency determined to be sufficient to meet the level of risk assessed by the agency.

(b) Reproduction. Reproduction of classified information shall be held to the minimum consistent with operational requirements. The following additional control measures shall be taken:

(1) Reproduction shall be accomplished by authorized persons knowledgeable of the procedures for classified reproduction;

(2) Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced to the extent required by operational needs, or to facilitate review for declassification;

(3) Copies of classified information shall be subject to the same controls as the original information; and

(4) The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified information is encouraged.

(c) Forms. The use of standard forms prescribed in Subpart H of this part is mandatory for all agencies that create and/or handle national security information.

(d) Redaction--(1) Policies and procedures. Classified information may be subject to loss, compromise, or unauthorized disclosure if it is not correctly redacted. Agencies shall establish policies and procedures for the redaction of classified information from documents intended for release. Such policies and procedures require the approval of the agency head and shall be sufficiently detailed to ensure that redaction is performed consistently and reliably, using only approved redaction methods that permanently remove the classified information from copies of the documents intended for release. Agencies shall ensure that personnel who perform redaction fully understand the policies, procedures, and methods and are aware of the vulnerabilities surrounding the process.

(2) Technical guidance for redaction. Technical guidance concerning appropriate methods, equipment, and standards for the redaction of classified electronic and optical media shall be issued by NSA.

Sec. 2001.46 Transmission.

(a) General. Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Directive.

(b) Dispatch. Agency heads shall establish procedures which ensure that:

(1) All classified information physically transmitted outside facilities shall be enclosed in two layers, both of which provide reasonable evidence of tampering and which conceal the contents. The inner enclosure shall clearly identify the address of both the sender and the intended recipient, the highest classification level of the contents, and any appropriate warning notices. The outer enclosure shall be the same except that no markings to indicate that the contents are classified shall be visible. Intended recipients shall be identified by name only as part of an attention line. The following exceptions apply:

(i) If the classified information is an internal component of a packable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information;

(ii) If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal classified information;

(iii) If the classified information is an item of equipment that is not reasonably packable and the shell or body is classified, it shall be concealed with an opaque enclosure that will hide all classified features;

(iv) Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and

(v) When classified information is hand-carried outside a facility, a locked briefcase may serve as the outer enclosure.

(2) Couriers and authorized persons designated to hand-carry classified information shall ensure that the information remains under their constant and continuous protection and that direct point-to-point delivery is made. As an exception, agency heads may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a combination padlock meeting Federal Specification FF-P-110, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

(c) Transmission methods within and between the U.S., Puerto Rico, or a U.S. possession or trust territory.

(1) Top Secret. Top Secret information shall be transmitted by direct contact between authorized persons; the Defense Courier Service or an authorized government agency courier service; a designated courier or escort with Top Secret clearance; electronic means over approved communications systems. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service or any other cleared or uncleared commercial carrier.

(2) Secret. Secret information shall be transmitted by:

(i) Any of the methods established for Top Secret; U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail, as long as the Waiver of Signature block on the U.S. Postal Service Express Mail Label shall not be completed; and cleared commercial carriers or cleared commercial messenger services. The use of street-side mail collection boxes is strictly prohibited; and

(ii) Agency heads may, when a requirement exists for overnight delivery within the U.S. and its Territories, authorize the use of the current holder of the GSA contract for overnight delivery of information for the Executive Branch as long as applicable postal regulations (39 CFR. Chapter I) are met. Any such delivery service shall be U.S. owned and operated, provide automated in-

transit tracking of the classified information, and ensure package integrity during transit. The contract shall require cooperation with government inquiries in the event of a loss, theft, or possible unauthorized disclosure of classified information. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified Communications Security Information, NATO, and foreign government information shall not be transmitted in this manner.

(3) Confidential. Confidential information shall be transmitted by any of the methods established for Secret information or U.S. Postal Service Certified Mail. In addition, when the recipient is a U.S. Government facility, the Confidential information may be transmitted via U.S. First Class Mail. However, Confidential information shall not be transmitted to government contractor facilities via first class mail. When first class mail is used, the envelope or outer wrapper shall be marked to indicate that the information is not to be forwarded, but is to be returned to sender. The use of streetside mail collection boxes is prohibited.

(d) Transmission methods to a U.S. Government facility located outside the U.S. The transmission of classified information to a U.S. Government facility located outside the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, shall be by methods specified above for Top Secret information or by the Department of State Courier Service. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system.

(e) Transmission of U.S. classified information to foreign governments. Such transmission shall take place between designated government representatives using the government-to-government transmission methods described in paragraph (d) of this section or through channels agreed to by the National Security Authorities of the two governments. When classified information is transferred to a foreign government or its representative a signed receipt is required.
(f) Receipt of classified information. Agency heads shall establish procedures which ensure that classified information is received in a manner which precludes unauthorized access, provides for inspection of all classified information received for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt of Top Secret and Secret information by an authorized recipient. As noted in paragraph (e) of this section, a receipt acknowledgment of all classified material transmitted to a foreign government or its representative is required.

Sec. 2001.47 Destruction.

Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by agency heads. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing. Agencies shall comply with the destruction equipment standard stated in Sec. 2001.42(b) of this Directive.

Sec. 2001.48 Loss, possible compromise or unauthorized disclosure.

(a) General. Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose.

(b) Cases involving information originated by a foreign government or another U.S. government agency. Whenever a loss or possible unauthorized disclosure involves the classified information

or interests of a foreign government agency, or another U.S. government agency, the department or agency in which the compromise occurred shall advise the other government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally will not be advised of any security system vulnerabilities that contributed to the compromise.

(c) Inquiry/investigation and corrective actions. Agency heads shall establish appropriate procedures to conduct an inquiry/investigation of a loss, possible compromise or unauthorized disclosure of classified information, in order to implement appropriate corrective actions, which may include disciplinary sanctions, and to ascertain the degree of damage to national security.

(d) Reports to ISOO. In accordance with section 5.5(e)(2) of the Order, agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under paragraphs 5.5(b)(1), (2), or (3) of the Order that:

(1) Is reported to oversight committees in the Legislative branch;
(2) May attract significant public attention;
(3) Involves large amounts of classified information; or
(4) Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(e) Department of Justice and legal counsel coordination. Agency heads shall establish procedures to ensure coordination with legal counsel whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the unauthorized disclosure of classified information. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, agency heads shall use established procedures to ensure coordination with:

(1) The Department of Justice, and
(2) The legal counsel of the agency where the individual responsible is assigned or employed.

Sec. 2001.49 Special Access Programs.

(a) General. The safeguarding requirements of this Directive may be enhanced for information in special access programs (SAP), established under the provisions of section 4.3 of the Order by the agency head responsible for creating the SAP. Agency heads shall ensure that the enhanced controls are based on an assessment of the value, critical nature, and vulnerability of the information.

(b) Significant interagency support requirements. Agency heads must ensure that a Memorandum of Agreement/Understanding is established for each SAP that has significant interagency support requirements, to appropriately and fully address support requirements and supporting agency oversight responsibilities for that SAP.

Sec. 2001.50 Telecommunications Automated Information Systems and Network Security.

Each agency head shall ensure that classified information electronically accessed, processed, stored or transmitted is protected in accordance with applicable national policy issuances identified in the Committee on National Security Systems (CNSS) issuances and the Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation.

Standard Security Forms

These standard security forms are used in administering the security classification programs in Government. Industry members should contact their contracting agency for information on how to obtain these forms. The majority of these items are available through the General Services Administration's (GSA) Federal Supply System. Some of the forms are available online at the GSA web site or can be obtained by calling 1(800) 525-8027.

- **SF-311 Agency Security Classification Management Program Data**
  The SF-311 is a data collection form that every Executive Branch agency submits on an annual basis to report the total number of original classification authorities, classification decisions, mandatory review requests, and declassification decisions for that particular agency. The data collected from these forms are reported in the Annual Report to the President.

- **SF-312 Classified Information Nondisclosure Agreement**
  The SF-312 is a contractual agreement between the U.S. Government and a cleared employee that must be executed as a condition of access to classified information. By signing the SF-312, the cleared employee agrees never to disclose classified information to an unauthorized person.

- **SF-700 Security Container Information**
  The SF-700 is a form that contains vital information about the security container in which it is located. This information includes location, container number, lock serial number, and contact information if the container is found open and unattended.

- **SF-701 Activity Security Checklist**
  The SF-701 is a checklist that is filled out at the end of each day to insure that classified materials are secured properly and allows for employee accountability in the event that irregularities are discovered.

- **SF-702 Security Container Check Sheet**
  The SF-702 provides a record of the names and times that persons have opened, closed and checked a particular container that holds classified information.

The following three cover sheets are placed on top of documents to clearly identify the classification level of the document and protect classified information from inadvertent disclosure.

- **SF-703 Top Secret Cover Sheet**
- **SF-704 Secret Cover Sheet**
- **SF-705 Confidential Cover Sheet**

The following labels are placed on various forms of U.S. Government property (i.e. CDs, diskettes, computers, etc.) to clearly identify the classification level of the information located in or on that property.

- **SF-706 Top Secret Label**
- **SF-707 Secret Label**
- **SF-708 Confidential Label**
- **SF-709 Classified Label**
- **SF-710 Unclassified Label**
  In a mixed environment in which classified and unclassified materials are being processed or stored, this label is used to identify media that contains unclassified information. It's function is to aid in distinguishing among those media that contain classified information in a mixed environment.

- **SF-711 Data Descriptor Label**
  Used to identify additional safeguarding controls pertaining to classified information that is stored or contained on various forms of media.

Education and Training Materials

Security education plays a critical role in the effectiveness of an agency's information security program. Below are links to security training aids.

The SF312- Briefing Booklet- Provides information about the "Classified Information Nondisclosure Agreement. It includes a brief discussion of the background and purpose of the SF 312; the text of pertinent legislative and executive authorities; a series of questions and answers on its implementation; and a copy of the SF 312. This can be found at:

http://www.archives.gov/isoo/training/standard-form-312.pdf

Executive Order 13526- Classified National Security Information (Effective Date: 12/29/2009)

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities. This can be found at:

http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

Executive Order 12968- Access to Classified Information
(Effective Date: 8/2/1995)

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life. Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security. This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information. This can be found at:

http://www.fas.org/sgp/clinton/eo12968.html

Executive Order 13549- Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities **Amendment to EO 13462** (Effective Date: 8/18/2010)

The purpose of this order is to ensure that security standards governing access to and safeguarding of classified material are applied in accordance with Executive Order 13526 of December 29, 2009 (''Classified National Security Information''), Executive Order 12968 of August 2, 1995, as amended (''Access to Classified Information''), Executive Order 13467 of June 30, 2008 (''Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information''), and Executive Order 12829 of January 6, 1993, as amended (''National Industrial Security Program''). This can be found at:

http://www.archives.gov/isoo/policy-documents/eo-13549.html

Executive Order 13549- Establishment of Pakistan and Afghanistan Support Office (Effective Date: 8/18/2010)

The purpose of the PASO shall be to perform the specific project of supporting executive departments and agencies in strengthening the governments in Afghanistan and Pakistan, enhancing the capacity of those governments to resist extremists, and maintaining an effective U.S. diplomatic presence in both countries. This can be found at:

http://www.federalregister.gov/articles/2010/08/23/2010-21020/establishment-of-pakistan-and-afghanistan-support-office#p-3