DoD 5200.1-PH-1

Assistant Secretary of Defense for
Command, Control, Communications, and
Intelligence (703) 695-2686

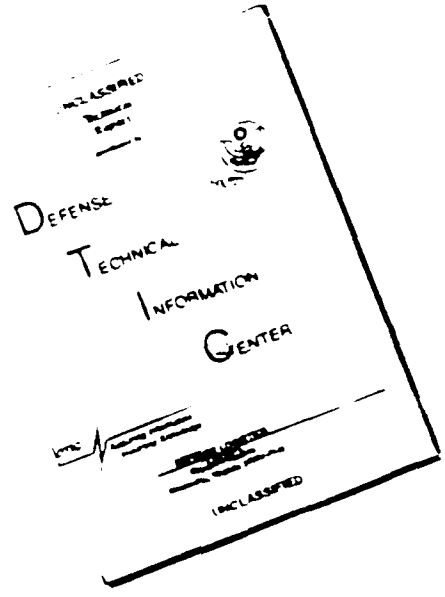
Department of Defense

Classified Information Nondisclosure Agreement (SF312) Briefing Pamphlet

Prepared by the Directorate of Security Plans and Programs
Office of the Deputy Under Secretary of Defense for Policy

March 1989

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

Foreword and Acknowledgment

March 1989

This pamphlet provides guidance on the SF 312 and supersedes DoD 5200.1-PH-1, "Classified Information Nondisclosure Agreement (SF 189)," dated July 1985. It is authorized by DoD Directive 5200.1, "DoD Information Security Program," and 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 implementation of the SF 312; a copy of the SF 312; and a sample indoctrination required by paragraph 2 of the SF 312.

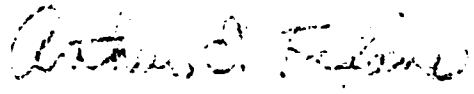
The guidance contained herein is derived from that promulgated by the Information Security Oversight Office (ISOO) which developed the SF 312 in collaboration with this office. ISOO has also produced a video on the SF 312 that is available by writing directly to that office at 18th and F Streets, N.W., Washington, D.C. 20405, telephone (202) 535-7251.

This pamphlet, including the sample indoctrination briefing, may be supplemented by security managers or supervisors with additional guidance that addresses problems or circumstances unique to the local organization.

This pamphlet should be available in the offices of those individuals, e.g., security managers, security education specialists, or supervisors who brief individuals about the protection of classified information and request execution of the SF 312. Moreover, all persons who are asked to execute the SF 312, or have executed it or its predecessors, the SF 189 or SF 189-A, should have the opportunity to receive or borrow a copy upon request.

For additional guidance, you should contact your security manager, supervisor, or legal counsel within your organization.

Comments of those using this booklet are invited and may be submitted to the Director of Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy, The Pentagon, Washington, D.C. 20301-2200, telephone autovon 225-2289/2686 or commercial (202) 695-2289/2686.



Arthur E. Fajans
Director
Security Plans and Programs

Table of Contents

Background and Purpose

As an employee of the Department of Defense or one of its contractors, licensees, or grantees who occupies a position which requires access to classified information, you have been the subject of a personnel security investigation. The purpose of this investigation was to determine your trustworthiness for access to classified information. When the investigation was completed, your employing or sponsoring department or agency granted you a security clearance based upon a favorable adjudication of the investigation results. By being granted a security clearance, you have met the first of three requirements necessary to have access to classified information.

The second requirement that you must fulfill is to sign a "Classified Information Nondisclosure Agreement," which is now the SF 312. The President established this requirement in a directive that states: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." The SF 312 is a contractual agreement between the U.S. Government and you, a cleared employee, in which you agree never to disclose classified information to an unauthorized person. Its primary purpose is to inform you of (1) the trust that is placed in you by providing you access to classified information; (2) your responsibilities to protect that information from unauthorized disclosure; and (3) the consequences that may result from your failure to meet those responsibilities. Additionally, by establishing the nature of this trust, your responsibilities, and the potential consequences of noncompliance in the context of a contractual agreement, if you violate that trust, the United States will be better able to prevent an unauthorized disclosure or to discipline you for such a disclosure by initiating a civil or administrative action.

The third and final requirement for access to classified information is the "need-to-know;" that is, you must have a need to know the information in order to perform your official duties. The holder of classified information to which you seek access is responsible for confirming your identify, your clearance, and your "need-to-know." As a holder of classified information, you are responsible for making these same determinations with respect to any individual to whom you may disclose it.

As a cleared employee you should receive, according to paragraph No. 2 of the SF 312, a "security indoctrination briefing concerning the nature and protection of classified information, including procedures to be followed in ascertaining whether other persons to whom you contemplate disclosing this information have been approved for access to it . . ." After you receive such a briefing, you should have a basic understanding of the following:

- What is classified information?
- How do you protect it?
- Who may have access to it?
- How does the classification system function?

The indoctrination briefing that follows may be used as a basic introduction to these points. Further, the ISOO video series on national security information provides answers to these questions and can be used for a security indoctrination or refresher briefing.

Sample Indoctrination Briefing

(Required by the Classified Information Nondisclosure Agreement (SF 312))

Background. As a result of President Reagan's concern that unauthorized disclosures of classified information threaten the security of our citizens, he directed that all persons authorized access to classified information shall be required to sign a nondisclosure agreement (NdA) as a condition of access. Therefore, those individuals who decline to sign an NdA shall be denied access to classified information, and appropriate action will be taken to revoke the security clearances of those declining individuals who already have access to classified information.

Nondisclosure Agreements. The new NdA is the SF 312 which is to be executed by all cleared Department of Defense (DoD) military and civilian personnel and contractor employees as a condition of access to classified information. The SF 312 is to be used in lieu of the SF 189, "Classified Information Nondisclosure Agreement," and the SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)." Previously executed copies of the SF 189 and SF 189-A remain valid and will be interpreted and enforced in a manner that is fully consistent with the interpretation and enforcement of the SF 312. Therefore, any cleared individual who has previously signed the SF 189 or the SF 189-A does not need to execute the SF 312. However, at the individual's discretion, he or she may elect to substitute a signed SF 312 for a previously signed SF 189 or SF 189-A.

Nature of Classified Information. Classified information is information that requires protection against unauthorized disclosure in the interest of national security (the national defense and foreign relations of the United States) and is classified under one of three designations, namely: "Top Secret," "Secret," or "Confidential," depending on the level of sensitivity. These are the only designations authorized to identify classified information.

"Top Secret" is applied only to information the unauthorized disclosure of which reasonably could be expected to cause "exceptionally grave damage" to the national security. Secret is applied only to information the unauthorized disclosure of which reasonably could be expected to cause "serious damage" to the national security. Confidential is applied only to information the unauthorized disclosure of which reasonably could be expected to cause "damage" to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, compromise of national-level cryptographic systems, exposure of some intelligence sources or methods, and substantial disruption of the capability of the National Command Authority to function in times of peace or crisis. Examples of "serious damage" and "damage" to national security are progressively less calamitous.

Note that security classification is not used for the sole purpose of concealing violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization, or agency, or to restrain competition.

The Classification of Information. Information may be classified in one to two ways: originally or derivatively.

Original Classification. Original classification is an initial determination by an original classification authority, who has been designated in writing, that information requires protection against unauthorized disclosure in the interest of national security. The original classification process includes both the determination of the need to protect the information and the placement of security markings to identify the information as classified.

In determining the need for classification, a two-step process must be satisfied. **First,** the information must fall within one or more of the following classification categories:

Military plans, weapons, or operations;

Vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security;

Foreign government information;

Intelligence activities (including special activities), or intelligence sources or methods

Foreign relations or foreign activities of the United States;

Scientific, technological, or economic matters relating to the national security;

United States Government programs for safeguarding nuclear materials or facilities;

Cryptology;

A confidential source; or

Other categories of information that are related to national security and that require protection against unauthorized disclosure as determined by the Secretary of Defense or Secretaries of the Military Departments; **and**

Secondly, the original classifier must determine that unauthorized dislcosure of the information reasonably could be expected to cause damage to the national security. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security. The original classifier therefore need not make a separate determination that these categories meet the damage criterion.

Derivative Classification. Derivative classification is just as its name implies--classification derived from another source. It is the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material in a manner that is consistent with the security markings of the source information. Only those DoD or contractor personnel who are required by their work to restate classified source information may classify derivatively.

Information is classified derivatively in one of two ways--through the use of a source document such as a security classification guide or other source document such as a report or correspondence. Information extracted from a classified report or correspondence to be incorporated into a new document is derivatively classified or not classified in accordance with the classification markings shown in the source document. The overall and internal markings of the source document should supply adequate classification guidance. If the source document is a classification guide, the derivative classification markings on the new document will be as prescribed by the guide.

Marking of Classified Information. At a minimum, classified documents must indicate 1) the highest level of classification; 2) the agency or office of origin; 3) the identity of the original classification authority or source document, as appropriate; and 4) if it can be determined, a date or event for declassification, otherwise, the indefinite declassification instruction will be indicated, i.e., "Originating Agency's Determination Required," or "OADR." In addition, each portion (e.g., titles, paragraphs) of a classified document must be marked to show level of classification, or that it is unclassified.

Challenges to Classification. If you as a holder of classified information have substantial reason to believe that the information has been classified improperly or unnecessarily, you must bring it to the attention of your security manager or the classifier of the information to bring about any necessary correction. The fact that you as a DoD civilian employee, contractor employee, or military member of the armed forces has issued a challenge to classification will not in any way result in or serve as a basis for adverse personnel action against you.

Protection of Classified Information. As a custodian of classified information, you have a personal, moral, and legal responsibility at all times to

protect classified information, whether oral or written, within your knowledge, possession, or control and for locking classified information in approved security containers or other equipment whenever it is not in use or under the direct supervision of authorized persons. Further, you must follow procedures which ensure that unauthorized persons do not gain access to classified information.

For example, classified material must not be discussed on the telephone, read, or discussed in public places. Don't be fooled by telephone callers who drop names or otherwise try to impress you with "urgent needs." Private codes or "talking around" classified information doesn't really fool anyone and should be strictly avoided. Further, many leaks of classified information result from conversations or interviews. Be very cautious in dealings with persons not authorized to have access to classified information. Remember, leaks may be just as damaging to our national security as outright espionage, and leakers should expect to be treated accordingly.

Care During Working Hours. Classified documents removed from storage must be kept under constant surveillance and face down or covered when not in use. Cover sheets used shall be Standard Forms 703, 704, and 705 for Top Secret, Secret, and Confidential documents, respectively.

Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, work-sheets, typewriter ribbons, working papers, floppy and hard disks, and other items containing classified information must be either destroyed immediately after they have served their purpose; or be given the same classification and secure handling as the classified information they contain.

Classified information may be processed by automated information systems but only by those systems that have been approved for such use.

Further, avoid routine reproduction of classified material. Classified material that is reproduced is subject to the same controls as the original document. Information classified "Secret" or higher may not be reproduced without authorization from an official who has been designated to grant such approval. You should note that Top Secret information must not be reproduced without the consent of the originator or higher authority.

Top Secret information is accounted for by a continuous chain of receipts; Secret information is controlled through administrative procedures such as the use of a receipt to ensure physical delivery in the absence of hand-to-hand transfer and the use of a record of receipt and dispatch regardless of the means used to ensure delivery of the information; and appropriate administrative controls are required to ensure that Confidential information is protected.

Memorize safe combinations and computer passwords. Never write a combination down on anything that is not securely stored in an approved security container or other approved security equipment. Further, classified information is not personal property and may not be removed from an activity's working area without specific authorization. Upon transfer or separation, we must return all classified information in our custody to our supervisor or security manager. Destroy all classified information that is no longer required for operational or record purposes. Storing unneeded classified information increases both cost and risk. Check with your security manager for the approved methods of destruction.

End-of-Day Security Checks. A system of security checks must be implemented at the close of each working day to ensure that all classified information is secure. Standard Form 701, "Activity Security Checklist," provides a systematic means to make a thorough end-of-day security inspection of a particular work area and shall be used to record such inspection. An integral part of the security inspection system is the security of all approved vaults, containers, and other approved equipment used for the storage of classified material. Standard Form 702, "Security Container Check Sheet," provides a record of the names and times that persons have opened, closed and checked a particular container or vault. Further, Standard Forms 701 and 702 must be annotated to reflect after-hours, weekend, and holiday activity.

Access. No person may have access to classified information unless that person has been determined to be trustworthy, and unless access is essential to the accomplishment of lawful and authorized government purposes, that is, the person has the appropriate security clearance and a demonstrated need-to-know. The final responsibility for deteriming whether a person's official duties require possession of or access to any element or item of classified information, and whether that person has been granted the appropriate security clearance by proper authority, rests upon the individual who has authorized possession, knowledge, or control of the information and **not** upon the prospective recipient. The possessor of the information is in the best position to determine whether a prospective recipient is cleared and has a need-to-know the information.

No one has a right to have access to classified information by possessing a security clearance alone but no need-to-know; solely by virtue of rank or position; or mere possession of a badge. Don't assume anything. Check identity, clearance, need-to-know, and ability to properly protect (or store) the information before passing classified information to anyone. Strictly limit distribution of papers and other media containing classified information. When in doubt, do not route. Avoid routine dissemination of classified material. Remember that each Top Secret document must be accompained by a disclosure record which indicates every person who has had access to the document.

Administrative Sanctions and Reporting Requirements. By failing to follow these rules and precautions, we expose ourselves to serious penalties if classified information is purposely or even negligently disclosed or compromised. Such penalties include but are not limited to a warning notice, reprimand, termination of classification authority, suspension without pay, forfeiture of pay, removal or discharge, fine and imprisonment.

You must immediately report any actual or suspected unauthorized disclosure or compromise of classified information to your security manager, applicable military service investigative or counterintelligence organization, or to the FBI. Do not even attempt to handle a security incident yourself--refer it to trained professionals.

Legislative and Executive Authorities

Title 18, United States Code

§641. Public money, property or records

Whoever embezzles, steals, purloins, or knowingly converts his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted--

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

Title 18, United States 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 not more than $10,000 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.

Title 18, United States Code

§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.

(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.

Title 18, United States Code

§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 process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes--

Shall be fined not more than $10,000 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.

Title 18, United States Code

§952. Diplomatic codes and correspondence

Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code, or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

Title 50, United States Code

§783. Offenses

(b) Communication of classified information by Government officer or employee

It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

TITLE VI -- PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION[1]

PROTECTION OF IDENTITIES OF CERTAIN UNITED STATES UNDERCOVER INTELLIGENCE OFFICERS, AGENTS, INFORMANTS, AND SOURCES

Sec. 601.(a) Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than $50,000 or imprisoned not more than ten years, or both.

(b) Whoever, as a result of having authorized access to classified information, learns the identity of a covert agent and intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than $25,000 or imprisoned not more than five years, or both.

(c) Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States, shall be fined not more than $15,000 or imprisoned not more than three years, or both.

---

[1]Title VI was added by the *Intelligence Identities Protection Act of 1982* (Public Law 97-200).

DEFENSES AND EXCEPTIONS

Sec. 602.(a) It is a defense to a prosecution under section 601 that before the commission of the offense with which the defendant is charged, the United States had publicly acknowledged or revealed the intelligence relationship to the United States of the individual the disclosure of whose intelligence relationship to the United States is the basis for the prosecution.

(b)(1) Subject to paragraph (2), no person other than a person committing an offense under section 601 shall be subject to prosecution under such section by virtue of section 2 or 4 of title 18, United States Code, or shall be subject to prosecution for conspiracy to commit an offense under such section.

(2) Paragraph (1) shall not apply (A) in the case of a person who acted in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, or (B) in the case of a person who has authorized access to classified information.

(c) It shall not be an offense under section 601 to transmit information described in such section directly to the Select Committee on Intelligence of the Senate or to the Permanent Select Committee on Intelligence of the House of Representatives.

(d) It shall not be an offense under section 601 for an individual to disclose information that solely identifies himself as a covert agent.

REPORT

Sec. 603.(a) The President, after receiving information from the Director of Central Intelligence, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives an annual report on measures to protect the identities of covert agents, and on any other matter relevant to the protection of the identities of covert agents.

(b) The report described in subsection (a) shall be exempt from any requirement for publication or disclosure. The first such report shall be submitted no later than February 1, 1983.

EXTRATERRITORIAL JURISDICTION

Sec. 604. There is jurisdiction over an offense under section 601 committed outside the United States if the individual committing the offense is a citizen of the United States or an alien lawfully admitted to the United States for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act).

PROVIDING INFORMATION TO CONGRESS

Sec. 605. Nothing in this title may be construed as authority to withhold information from the Congress or from a committee of either House of Congress.

DEFINITIONS

Sec. 606. For the purposes of this title:

(1) The term "classified information" means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

(2) The term "authorized", when used with respect to access to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.

(3) The term "disclose" means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

(4) The term "covert agent" means--

(A) an officer or employee of an intelligence agency or a member of the Armed Forces assigned to duty with an intelligence agency--

(i) whose identity as such an officer, employee, or member is classified information, and

(ii) who is serving outside the United States or has within the last five years served outside the United States; or

(B) a United States citizen whose intelligence relationship to the United States is classified information, and--

(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or

(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

(5) The term "intelligence agency" means the Central Intelligence Agency, a foreign intelligence component of the Department of Defense, or the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation.

(6) The term "informant" means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

(7) The terms "officer" and "employee" have the meanings given such terms by section 2104 and 2105, respectively, of title 5, United States Code.

(8) The term "Armed Forces" means the Army, Navy, Air Force, Marine Corps, and Coast Guard.

(9) The term "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(10) The term "pattern of activities" requires a series of acts with a common purpose or objective.

Title 3 -- Executive Order 12356 of April 2, 1982
3 CFR 66 (1982 Comp.); 47 Fed. Reg. 14874

The President National Security Information

TABLE OF CONTENTS

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Part 1

Original Classification

Section 1.1 Classification Levels.

(a) National security information (hereinafter "classified information") shall be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information.

(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

Sec. 1.2 Classification Authority.

(a) Top Secret. The authority to classify information originally as Top Secret may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the **Federal Register**; and

(3) officials delegated this authority pursuant to Section 1.2(d).

(b) Secret. The authority to classify information originally as Secret may be exercised only by:

(1) agency heads and officials designated by the President in the **Federal Register**;

(2) officials with original Top Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(c) Confidential. The authority to classify information originally as Confidential may be exercised only by:

(1) agency heads and officials designated by the President in the **Federal Register**;

(2) officials with original Top Secret or Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(d) Delegation of Original Classification Authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a), provided that official has been delegated original Top Secret classification authority by the agency head.

(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a), provided that official has been delegated original Secret classification authority by the agency head.

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a), provided that official has been delegated original classification authority by the agency head.

(5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.

(e) Exceptional Cases. When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.3 Classification Categories.

(a) Information shall be considered for classification if it concerns:

(1) military plans, weapons, or operations;

(2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) foreign government information;

(4) intelligence activities (including special activities), or intelligence sources or methods;

(5) foreign relations or foreign activities of the United States;

(6) scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safeguarding nuclear materials or facilities;

(8) cryptology;

(9) a confidential source; or

(10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

Sec. 1.4 Duration of Classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

Sec. 1.5 Identification and Markings.

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

(1) one of the three classification levels defined in Section 1.1;

(2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;

(3) the agency and office of origin; and

(4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

Sec. 1.6 Limitations on Classification.

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a), or an official with original Top Secret classification authority.

Part 2

Derivative Classification

Sec. 2.1 Use of Derivative Classification.

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

Sec. 2.2 Classification Guides.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a); and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

Part 3

Declassification and Downgrading

Sec. 3.1 Declassification Authority.

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a).

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.

Sec. 3.2 Transferred Information.

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

Sec. 3.3 Systematic Review for Declassification.

(a) The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.

(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.4 Mandatory Review for Declassification.

(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:

(1) the request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and

(2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized under applicable law.

(d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request.

(e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

Part 4

Safeguarding

Sec. 4.1 General Restrictions on Access.

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

Sec. 4.2 Special Access Programs.

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence.

(b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.

Sec. 4.3 Access by Historical Researchers and Former Presidential Appointees.

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:

(1) are engaged in historical research projects, or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under Section 4.3(a) may be granted only if the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and

(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

Implementation and Review

Sec. 5.1 Policy Direction.

(a) The National Security Council shall provide overall policy direction for the information security program.

(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2 Information Security Oversight Office.

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

(b) The Director shall:

(1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;

(2) oversee agency actions to ensure compliance with this Order and implementing directives;

(3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;

(7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

Sec. 5.3 General Responsibilities.

Agencies that originate or handle classified information shall:

(a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;

(b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the **Federal Register** to the extent that these regulations affect members of the public;

(c) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs; and

(d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

Sec. 5.4 Sanctions.

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official designated under Section 5.3(a) so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they:

(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;

(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) Each agency head or the senior official designated under Section 5.3(a) shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b)(1) or (2) occurs.

Part 6

General Provisions

Sec. 6.1 Definitions.

(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).

(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(d) "Foreign government information" means:

(1) 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

(2) 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 element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(e) "National security" means the national defense or foreign relations of the United States.

(f) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both be held in confidence.

(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

Sec. 6.2 General.

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. 12065 of June 28, 1978, as amended, is revoked as of the effective date of this Order.

(e) This Order shall become effective on August 1, 1982.

Ronald Reagan

THE WHITE HOUSE
April 2, 1982.

Implementing Rule of the
"Classified Information Nondislosure Agreement"
Section 2003.20 of Title 32, Code of Federal Regulations
as published in Vol. 53, *Federal Register*, p. 38278
September 29, 1988

32 CFR Part 2003 is amended as follows:

PART 2003 -- NATIONAL SECURITY INFORMATION -- STANDARD FORMS

1. The authority citation for 32 CFR Part 2003 continues to read:

Authority: Sec. 5.2(b)(7) of E.O. 12356.

Subpart B - Prescribed Forms

2. Section 2003.20 is revised to read as follows:

§2003.20 Classified Information Nondisclosure Agreement: SF 312; Classified Information Nondisclosure Agreement: SF 189; Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government): SF 189-A.

(a) SF 312, SF 189, and SF 189-A are nondisclosure agreements between the United States and an individual. The prior execution of at least one of these agreements, as appropriate, by an individual is necessary before the United States Government may grant that individual access to classified information. From the effective date of this rule, the SF 312 shall be used in lieu of both the SF 189 and the SF 189-A for this purpose. In any instance in which the language in the SF 312 differs from the language in either the SF 189 or SF 189-A, agency heads shall interpret and enforce the SF 189 or SF 189-A in a manner that is fully consistent with the interpretation and enforcement of the SF 312.

(b) All employees of executive branch departments, and independent agencies or offices, who have not previously signed the SF 189, must sign the SF 312 before being granted access to classified information. An employee who has previously signed the SF 189 is permitted, at his or her own choosing, to substitute a signed SF 312 for the SF 189. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(c) All Government contractor, licensee, and grantee employees, or other non-Government personnel requiring access to classified information in the performance of their duties, who have not previously signed either the SF 189 or the SF 189-A, must sign the SF 312 before being granted access to classified information. An employee who has previously signed either the SF 189 or the SF 189-A is permitted, at his or her own choosing, to substitute a signed SF 312 for either the SF 189 or the SF 189-A. In these instances, agencies, with the cooperation of the pertinent contractor, licensee or grantee, shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(d) Agencies may require other persons, who are not included under paragraphs (b) or (c) of this section, and who have not previously signed either the SF 189 or the SF 189-A, to execute SF 312 before receiving access to classified information. A person in such circumstances who has previously signed either the SF 189 or the SF 189-A is permitted, at his or her own choosing, to substitute a signed SF 312 for either the SF 189 or the SF 189-A. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(e) The use of the "Security Debriefing Acknowledgement" portion of the SF 312 is optional at the discretion of the implementing agency.

(f) An authorized representative of a contractor, licensee, grantee, or other non-Government organization, acting as a designated agent of the United States, may witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States. Also, an employee of a United States agency may witness the execution of the SF 312 by an employee, contractor, licensee or grantee of another United States agency, provided that an authorized United States Government official or, for non-Government employees only, a designated agent of the United States subsequently accepts by signature the SF 312 on behalf of the United States.

(g) The provisions of the SF 312, the SF 189, and the SF 189-A do not supersede the provisions of Section 2302, Title 5, United States Code, which pertain to the protected disclosure of information by Government employees, or any other laws of the United States.

(h) (1) *Modification of the SF 189.*

The second sentence of Paragraph 1 of every executed copy of the SF 189 is clarified to read:

As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1(c) and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security.

(2) *Scope of "classified information".*

As used in the SF 312, the SF 189, and the SF 189-A, "classified information" is marked or unmarked classified information, including oral communications; and unclassified information that meets the standards for classification and is in the process of a classification determination, as provided in Sections 1.1(c) and 1.2(e) of Executive Order 12356 or any other statute or Executive order that requires interim protection for certain information while a classification determination is pending. "Classified information" does not include unclassified information that may be subject to possible classification at some future date, but is not currently in the process of a classification determination.

(3) *Basis for liability.*

A party to the SF 312, SF 189 or SF 189-A may be liable for disclosing "classified information" only if he or she knows or reasonably should know that: (i) the marked or unmarked information is classified, or meets the standards for classification and is in the process of a classification determination; and (ii) his or her action will result, or reasonably could result in the unauthorized disclosure of that information. In no instance may a party to the SF 312, SF 189 or SF 189-A be liable for violating its nondisclosure provisions by disclosing information when, at the time of the disclosure, there is no basis to suggest, other than pure speculation, that the information is classified or in the process of a classification determination.

(i) *Points of clarification.*

(1) As used in Paragraph 3 of SF 189 and SF 189-A, the word "indirect" refers to any situation in which the knowing, willful or negligent action of a party to the agreement results in the unauthorized disclosure of classified information even though the party to the agreement does not directly communicate, deliver or transmit classified information to a person who is not authorized to receive it.

(2) As used in Paragraph 7 of SF 189, "information" refers to "classified information," exclusively.

(3) As used in the third sentence of Paragraph 7 of SF 189 and SF 189-A, the words "all materials which have, or may have, come into my possession," refer to "all classified materials which have or may come into my possession," exclusively.

(j) Each agency must retain its executed copies of the SF 312, SF 189, and SF 189-A in file systems from which the agreements can be expeditiously retrieved in the event that the United States must seek their enforcement. The copies or legally enforceable facsimiles of them must be retained for 50 years following their date of execution. An agency may permit its contractors, licensees and grantees to retain the executed agreements of their employees during the time of employment. Upon the termination of employment, the contractor, licensee or grantee shall deliver the SF 312, SF 189, or SF 189-A of that employee to the Government agency primarily responsible for his or her classified work.

(k) Only the National Security Council may grant an agency's request for a waiver from the use of the SF 312. To apply for a waiver, an agency must submit its proposed alternative nondisclosure agreement to the Director of ISOO, along with a justification for its use. The Director of ISOO will request a determination about the alternative agreement's enforceability from the Department of Justice prior to making a recommendation to the National Security Council. An agency that has previously received a waiver from the use of the SF 189 or the SF 189-A need not seek a waiver from the use of the SF 312.

(l) The national stock number for the SF 312 is 7540-01-280-5499.

Questions and Answers

List of Questions

Question 1: What is the Information Security Oversight Office?

Answer: Under Executive Order 12356, "National Security Information," the Information Security Oversight Office (ISOO) is responsible for monitoring the information security programs of all executive branch departments and agencies that create or handle national security information. In National Security Decision Directive No. 84, March 11, 1983, the President directed ISOO to develop and issue a standardized classified information nondisclosure agreement to be executed by all cleared persons as a condition of access to classified information.

Question 2: What is the purpose of the SF 312?

Answer: The primary purpose of the SF 312 is to inform employees of (a) the trust that is placed in them by providing them access to classified information; (b) their responsibilities to protect that information from unauthorized disclosure; and (c) the consequences that may result from their failure to meet those responsibilities. Secondly, by establishing the nature of that trust, those responsibilities, and those consequences in the context of a contractual agreement, if that trust is violated, the United States will be in a better position to prevent an unauthorized disclosure or to discipline an employee responsible for such a disclosure by initiating a civil or administrative action.

Question 3: Upon what legal authority is the SF 312 based?

Answer: The direct legal bases for the issuance of SF 312 are Executive Order 12356, in which the President authorizes the Director of ISOO to issue standardized security forms; and National Security Decision Directive No. 84 (NSDD 84), in which the President directs ISOO to issue a standardized classified information nondisclosure agreement. Both E.O. 12356 and NSDD 84 are based on the President's constitutional responsibilities to protect national security information. These responsibilities derive from the President's powers as Chief Executive, Commander-in-Chief, and the principal architect of United States foreign policy.

Nondisclosure agreements have consistently been upheld by the Federal courts, including the Supreme Court, as legally binding and constitutional. At every stage of the development and implementation of the SF 312 and its predecessors, the SF 189 and the SF 189-A, experts in the Department of Justice have reviewed their constitutionality and enforceability under existing law. The most recent litigation over the SF 189 resulted in a decision that upheld its basic constitutionality and legality.

Question 4: Who must sign the SF 312?

Answer: As provided in National Security Decision Directive No. 84, dated March 11, 1983: "All persons with authorized access to classified information

shall be required to sign a nondisclosure agreement as a condition of access." Therefore, each person at the time that he or she is cleared for access to classified information, or each person who has been cleared previously and continues to require access to classified information must sign the SF 312, unless he or she has previously executed one or more of the following:

(a) The SF 189, for cleared employees in both Government and industry;

(b) The SF 189-A, for cleared employees within industry; or

(c) A nondisclosure agreement for which the National Security Council has granted a waiver from the use of the SF 312, the SF 189 or the SF 189-A, as provided in 32 CFR §2003.20.

By tradition and practice, United States officials who hold positions prescribed by the Constitution of the United States are deemed to meet the standards of trustworthiness for eligibility for access to classified information. Therefore, the President, the Vice President, Members of Congress, Supreme Court Justices, and other federal judges appointed by the President and confirmed by the Senate need not execute the SF 312 as a condition of access to classified information.

Question 5: Are all Members of Congress entitled to unlimited access to classified information?

Answer: No. Access to classified information is a function of three pre-conditions: (1) A determination of a person's trustworthiness, i.e., the security clearance; (2) the signing of an approved nondisclosure agreement; and (3) the exercise of the "need-to-know" principle, i.e., access is necessary in order to perform one's job. Members of Congress, as constitutionally elected officials, are not ordinarily subject to clearance investigations nor does ISOO's rule implementing the SF 312 require that Members of Congress sign the SF 312 as a condition of access to classified information. Members of Congress are not exempt, however, from fulfilling the "need-to-know" requirement. They are not inherently authorized to receive all classified information, but agencies provide access as is necessary for Congress to perform its legislative functions, for example, to members of a committee or subcommittee that oversees classified executive branch programs. Frequently, access is governed in these situations by ad hoc agreements or rules to which the agency head and the committee chairman agree.

The three basic requirements for access to classified information mentioned in the opening paragraph apply to congressional staffs as well as executive branch employees. ISOO's regulation implementing the SF 312 provides that agency heads may use it as a nondisclosure agreement to be signed by non-executive branch personnel, such as congressional staff members. However, agency heads are free to substitute other agreements for this purpose.

Question 6: Is an employee who signed an SF 312, SF 189 or SF 189-A in a prior position required to sign an SF 312 in a new position that also involves access to classified information?

Answer: The SF 312 and its predecessors have been purposely designed so that new nondisclosure agreements need not be signed upon changing jobs. Therefore, ordinarily the answer is no. However, if the location and retrieval of a previously signed agreement cannot be accomplished in a reasonable amount of time or with a reasonable amount of effort, the execution of the SF 312 may be practicable or even necessary. Also, a person who has signed the SF 189-A, which was designed exclusively for non-Government employees, would be required to sign the SF 312 if he or she began working for a Government agency in a position that required access to classified information.

Question 7: Should a person who does not now have a security clearance but who may very well have such a clearance in the future sign the SF 312?

Answer: No. The SF 312 should be signed only by persons who already have a security clearance or are being granted a security clearance at that time. It is inappropriate to have any uncleared person sign the SF 312, even if that person may have a need to be cleared in the near future.

Question 8: Should a person who has a security clearance but has no occasion to have access to classified information be required to sign the SF 312?

Answer: Since every cleared person must sign a nondisclosure agreement, the routine answer to this question is "yes." However, there are employees who have questioned executing a nondisclosure agreement on the basis that they have not had access to classified information over a lengthy period of time. Persons who do not require access to classified information should not have or retain security clearances. Therefore, the agency or contractor in such a situation should first determine the need for the retention of the security clearance. If its retention is unnecessary or speculative, the clearance should be withdrawn through established procedures and the employee should not sign the SF 312. If the agency or contractor determines a legitimate, contemporaneous need for the employee's clearance, the employee must sign the SF 312.

Question 9: Must an employee execute the SF 312 at the time he or she is briefed about the requirement to do so?

Answer: No. An employee who requests additional time to consider his or her decision to execute the SF 312 should be provided a reasonable amount of time to do so. The particular circumstances of the situation must govern what is a

reasonable amount of time. In every situation, however, the agency or contractor should give the employee a written determination of the additional time that he or she shall have to make that decision. Also, in any situation in which there is a delay in the execution of the SF 312, the employee should be advised of the criminal, civil or administrative consequences that may result from the unauthorized disclosure of classified information, even though the individual has not yet signed the nondisclosure agreement.

Question 10: What happens if a person who has not signed either the SF 189 or SF 189-A refuses to sign the SF 312?

Answer: As provided by presidential directive, the execution of an approved nondisclosure agreement shall be a condition of access to classified information. Therefore, an agency shall take those steps that are necessary to deny a person who has not executed an approved nondisclosure agreement any further access to classified information. In accordance with agency regulations and procedures, the affected party's security clearance shall either be withdrawn or denied. For purposes of meeting this condition for access, the approved nondisclosure agreements include any of the following:

(a) The SF 312, for cleared employees in both Government and industry;

(b) The SF 189, for cleared employees in both Government and industry;

(c) The SF 189-A, for cleared employees within industry; or

(d) A nondisclosure agreement for which the National Security Council has granted a waiver from the use of the SF 312, the SF 189 or the SF 189-A, as provided in 32 CFR §2003.20.

While the refusal to sign a required nondisclosure agreement directly affects the withdrawal or denial of a security clearance, this, in turn, may also lead to adverse employment actions, including removal. The agency or contractor should advise each affected employee of the particular consequences that will or may result from his or her refusal to sign a required nondisclosure agreement.

Question 11: How does the SF 312 differ from the SF 189 and SF 189-A?

Answer: The most obvious difference between the SF 312 and the SF 189 or SF 189-A is that the SF 312 has been designed to be executed by both Government and non-Government employees. The SF 312 differs from the SF 189 and SF 189-A in several other ways as well.

First, the term "classifiable information," which has now been removed from paragraph 1 of the SF 189 by regulation, does not appear in the SF 312.

Second, the modifiers "direct" and "indirect," which appear in Paragraph 3 of both the SF 189 and SF 189-A, do not appear in the new nondisclosure agreement.

Third, the "Security Debriefing Acknowledgement," which appears in the SF 189-A but not the SF 189, is included in the SF 312. Its use is optional at the discretion of the implementing agency.

Fourth, the SF 312 includes specific references to marked or unmarked classified information and information that is in the process of a classification determination. These references have now been added to the SF 189 by regulation.

Fifth, the SF 312 specifically references a person's responsibility in situations of uncertainty to confirm the classification status of information before disclosure.

The SF 312 also contains several other editorial changes which clarify perceived ambiguities in the predecessor forms. Notwithstanding these changes, the SF 312 does not in any way differ from the SF 189 and SF 189-A with respect to the substance of the classified information that each has been designed to protect.

Question 12: For purposes of the SF 312, what is "classified information?"

Answer: As used in the SF 312, the SF 189, and the SF 189-A, "classified information" is marked or unmarked classified information, including oral communications; and unclassified information that meets the standards for classification and is in the process of a classification determination, as provided in Sections 1.1(c) and 1.2(e) of Executive Order 12356 or under any other Executive order or statute that requires interim protection for certain information while a classification determination is pending. "Classified information" does not include unclassified information that may be subject to possible classification at some future date, but is not currently in the process of a classification determination.

The current Executive order and statute under which "classified information," as used in the SF 312, is generated are Executive Order 12356, "National Security Information," and the Atomic Energy Act of 1954, as amended.

Question 13: What is the threshold of liability for violating the nondisclosure provisions of the SF 312?

Answer: A party to the SF 312, SF 189 or SF 189-A may be liable for disclosing "classified information" only if he or she knows or reasonably should know that:

(a) the marked or unmarked information is classified, or meets the standards for classification and is in the process of a classification determination; and (b) his or her action will result, or reasonably could result in the unauthorized disclosure of that information. In no instance may a party to the SF 312, SF 189 or SF 189-A be liable for violating its nondisclosure provisions by disclosing information when, at the time of the disclosure, there is no basis to suggest, other than pure speculation, that the information is classified or in the process of a classification determination.

Question 14: May the language of the SF 312 be altered to suit the preferences of an individual signer?

Answer: No. The SF 312 as drafted has been approved by the National Security Council as meeting the requirements of NSDD 84, and by the Department of Justice as an enforceable instrument in a court of law. An agency may not accept an agreement in which the language has been unilaterally altered by the signer.

Question 15: Why are there separate entries on the SF 312 for the person who witnesses its execution by the employee and the person who accepts the agreement on behalf of the Government? Must different persons perform each function?

Answer: In most circumstances, one person may serve as both the witness and acceptor of the SF 312, and, in these cases, both entries should be affixed to the SF 312 at the time of execution. Different persons must perform each function only when a person authorized to witness the execution of the SF 312 in a particular situation is not authorized to accept it on behalf of the United States in that same situation. Then, the entry as witness should be affixed to the SF 312 at the time of execution, and the entry as acceptor should be affixed by an authorized person as soon as possible after execution.

Any executive branch employee may *witness* the execution of the SF 312 by a Government or non-Government employee.

An agency employee specifically authorized to do so may *accept* on behalf of the United States an SF 312 executed by either an employee of that same agency or a non-Government employee whose clearance is granted through that agency.

An authorized representative of a contractor, licensee, grantee, or other non-Government organization, designated to act as an agent of the United States, may *witness and accept* an SF 312 executed by an employee of that same organization.

Question 16: Does the SF 312 conflict with the "whistleblower" statute?

Answer: The SF 312 does not conflict with the "whistleblower" statute (5 U.S.C. §2302). The statute does not protect employees who disclose classified information without authority. If an employee knows or reasonably should know that information is classified, provisions of the "whistleblower statutes" should not protect that employee from the consequences of an unauthorized disclosure.

In addition, Executive Order 12356, Sec. 1.6(a), specifically prohibits classification "in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security." This provision was included in the Order to help prevent the classification of information that would most likely be the concern of whistleblowers.

Finally, there are remedies available to whistleblowers that don't require the unauthorized disclosure of classified information. There are officials within the Government who are both authorized access to classified information and who are responsible for investigating instances of reported waste, fraud, and abuse. Further, each agency has designated officials to whom challenges to classification may be addressed or to whom a disclosure of classified information is authorized. For example, within the Department of Defense emlpoyees are now required to challenge the classification of information that they believe is not properly classified. Special procedures have been established to expedite decisions on these challenges.

Question 17: Must a signatory to the SF 312 submit any materials that he or she contemplates publishing for prepublication review by the employing or former employing agency?

Answer: No. There is no explicit or implicit prepublication review requirement in the SF 312, as there is none in the SF 189 and SF 189-A. However, if an individual who has had access to classified information is concerned that something he or she has prepared for publication may contain classified information, that individual should be encouraged to submit it to his or her current or last employing agency for a voluntary review. In this way the individual will minimize the possibility of a subsequent action against him or her as a result of an unauthorized disclosure.

Question 18: Why do the obligations to protect classified information under the SF 312 extend beyond the duration of an employee's clearance?

Answer: The terms of the SF 312 specifically state that all obligations imposed on the signer "apply during the time [the signer is] granted access to classified information, and at all times thereafter." This provision recognizes that the duration of the national security sensitivity of classified information rarely has any relationship to the duration of any particular individual's clearance. The injury to the United States that may result from an unauthorized disclosure is not dependent on the current status of the discloser.

The obligations imposed by the SF 312 apply to classified information. If particular information has been declassified, under the terms of the SF 312 there is no continuing nondisclosure obligation on the part of the signer. Further, the signer of the SF 312 may initiate a mandatory review request to seek the declassification of specified classified information, including information to which the signer has access.

Question 19: If information that a signer of the SF 312 knows to have been classified appears in a public source, for example, in a newspaper article, may the signer assume that the information has been declassified and disseminate it elsewhere?

Answer: No. Information remains classified until it has been officially declassified. Its disclosure in a public source does not declassify the information. Of course, merely quoting the public source in the abstract is not a second unauthorized disclosure. However, before disseminating the information elsewhere or confirming the accuracy of what appears in the public source, the signer of the SF 312 must confirm through an authorized official that the information has, in fact, been declassified. If it has not, further dissemination of the information or confirmation of its accuracy is also an unauthorized disclosure.

Question 20: What civil and administrative actions may the Government take to enforce the SF 312?

Answer: Among the civil actions that the Government may bring in Federal court are the application for a court order enjoining the publication or other disclosure of classified information; suits for money damages to recompense the United States for the damages caused by an unauthorized disclosure; and suits to require the forfeiture to the United States of any payments or other monetary or property gains that have resulted or may result from an unauthorized disclosure.

The scope of prospective administrative actions depends on whether the person alleged to have violated the SF 312 is a Government or non-Government employee. A Government employee would be subject to the entire range of administrative sanctions and penalties, including reprimand, suspension, demotion or removal, in addition to the likely loss of the security clearance.

In situations involving an unauthorized disclosure by a non-Government employee, the action will focus on the relationship between the Government and the organization that employs the individual. The Government cannot remove or otherwise discipline a non-Government employee, but it can, and in all likelihood will revoke the security clearance of that employee, and prevent the employing organization from using that employee on classified projects. The Government may also move against the employing organization in accordance with the terms of their relationship. For example, in a Government contract situation, the Government may move to terminate the contract or to seek monetary damages from the contractor, based on the terms of the contract.

Although the enforcement of the SF 312, as a contractual instrument, is limited to civil or administrative actions, the Government may also criminally prosecute individuals or organizations that are alleged to have violated a criminal statute that involves the unauthorized disclosure of classified information. These criminal statutes are listed in the SF 312, and are reprinted in this booklet.

Question 21: How long must executed copies of the SF 312 be retained? Where must they be stored? Can they be retained in a form other than the original paper copy?

Answer: The originals or legally enforceable facsimiles of the SF 312 must be retained for 50 years following the date of execution. Ordinarily, microforms and other reproductions are legally enforceable in the absence of the originals. Each agency must retain its executed copies of SF 312 in a file system from which the agreement can be expeditiously retrieved in the event that the United States must seek their enforcement. Official personnel files, both for civilian and military service, ordinarily are not scheduled for preservation for a sufficient period of time to allow them to be used for this purpose.

The retention of the nondisclosure agreements by contractors shall be governed by instructions issued by the Defense Investigative Service or other agency that is responsible for security administration of the contractor's classified contracts. These instructions must take into account the retention and retrieval standards discussed above.

Question 22: May the signer keep a copy of the executed SF 312?

Answer: Ordinarily, a signer of the SF 312 who requests a copy of the executed form may keep one. Only in the extraordinary situation in which one of the signatures on the agreement reveals a classified relationship, resulting in the classification of that particular form, may the signer not keep a copy.

Copy of the SF 312

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1(c) and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it, or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and §952, Title 18, United States Code, §the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse)

NSN 7540-01-280-5499

STANDARD FORM 312 (9-88)
Prescribed by GSA/ISOO
32 CFR 2003 E.O. 12356

10. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *Section 783(b), Title 50, United States Code, the Intelligence Identities Protection Act of 1982, Executive Order 12356 or its successor, and Section 2003.20, Title 32, Code of Federal Regulations so that I may read them at this time, if I so choose.

WITNESS	ACCEPTANCE
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.	THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT
SIGNATURE / DATE	SIGNATURE / DATE
NAME AND ADDRESS (Type or print)	NAME AND ADDRESS (Type or print)

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE / DATE

NAME OF WITNESS (Type or print) / SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-88)

Notes

Security Manager _____

Telephone _____

Notes

Notes

Notes

☆ U. S. Government Printing Office: 1989 - 238-362 (00402)