Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet

Reviewed August 2016

INTRODUCTION

This booklet provides you with information about the "Classified Information Nondisclosure Agreement," also known as the "SF 312." It includes a brief discussion of the background and purpose of the SF 312; the text of pertinent legislative and executive authorities; a series of questions and answers on its implementation; and a copy of the SF 312. Each organization may wish to supplement this booklet with additional guidance that addresses problems or circumstances unique to it.

This booklet should be available in the offices of those persons who brief individuals about the SF 312, e.g., security managers, security education specialists, or supervisors. Further, 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, please contact your security manager, supervisor or legal counsel within your organization. If questions concerning the SF 312 cannot be answered within your organization, please bring them to the attention of ISOO, 700 Pennsylvania Avenue, N.W., Washington, D.C. 20408, telephone number (202) 219-5250.

BACKGROUND AND PURPOSE

As an employee of the Federal Government 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 determination 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," the SF 312. The President first 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." This requirement is reiterated in the executive order on classified national security information. 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 identity, 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?

A variety of educational materials are available that provide answers to these questions. Several training methods may be used to convey this information, including briefings, interactive videos, and dissemination of instructional materials. Contact your security manager for more information.

LEGISLATIVE AND EXECUTIVE AUTHORITIES

Title 18, United States Code

Section 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

Sec. 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 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 concerned 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, 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; orv

(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

Section 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 in 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

Section 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 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

Section 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

Section 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 5, United States Code

Section 2302. Prohibited personnel practices

(b) Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority--

(8) take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment because of

(A) any disclosures of information by an employee or applicant which the employee or applicant reasonably believes evidences--

(i) a violation of any law, rule, or regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, if such disclosure is not specifically prohibited by law and if such information is specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or

(B) any disclosure to the Special Counsel of the Merit Systems Protection Board, or to the Inspector General of an agency or another employee rated by the head of the agency to receive such disclosures, of information the employee or applicant reasonably believes evidences--

(i) a violation of any law, rule, or regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health and safety;

Title 5, United States Code

Section 7211. Employees' right to petition Congress

The right of employees, individually or collectively, to petition Congress or a Member of Congress, or to furnish information to either House of Congress, or to a committee or Member thereof, may not be interfered with or denied.

Title 10, United States Code

Section 1034. Communicating with a Member of Congress or Inspector General; prohibition on retaliatory personnel actions

(a) Restricting communications with Members of Congress and Inspector General prohibited.

(1) No person may restrict a member of the armed forces in communicating with a Member of Congress or an Inspector General.

(2) Paragraph (1) does not apply to a communication that is unlawful.

(b) Prohibition of retaliatory personnel actions. No person may take (or threaten to take) an unfavorable personnel action, or withhold (or threaten to withhold) a favorable personnel action, as a reprisal against a member of the armed forces for making or preparing a communication to a Member of Congress or an Inspector General that (under subsection (a)) may not be restricted. Any action prohibited by the preceding sentence (including the threat to take any action and the withholding or threat to

withhold any favorable action) shall be considered for the purposes of this section to be a personnel action prohibited by this subsection.

TITLE VI-- PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION*

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

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.

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 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 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 in 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 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.

(6) 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.

Executive Order 12958 of April 17, 1995
60 Fed. Reg. 19825
CLASSIFIED NATIONAL SECURITY INFORMATION

Implementing Rule of the "Classified Information Nondisclosure Agreement"

Subpart B--Prescribed Forms

Sec. 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 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 is 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 Section 1.1(c) and 1.2(e) of Executive Order 12356 or any other 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.

(4) Modification of the SF 312, SF 189, and SF 189-A

(i) Each executed copy of the SF 312, SF 189 and SF 189-A, whether executed prior to or after the publication of this rule, is amended to include the following Paragraphs 10 and 11.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302 (b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. 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 the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

(ii) The first sentence of Paragraph 7 of each executed copy of SF 312, SF 189 and SF 189-A, whether executed prior to or after the publication of this rule, is amended to read:

I understand that all classified information to which I have access or 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.

The second sentence of Paragraph 7 of each executed copy of the SF 312 (September 1988 version), SF 189 and SF 189-A, which reads, "I do not now, nor will I ever, possess any right, interest, title or claim whatsoever to such information," and whether executed prior to or after the publication of this rule is deleted.

(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 3-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 an agreement can be expeditiously retrieved in the event that the United States must seek its enforcement or a subsequent employer must confirm its prior execution. The original, or a legally enforceable facsimile that is retained in lieu of the original, such as microfiche, microfilm, computer disk, or electronic storage medium, must be retained for 50 years following its date of execution. For agreements executed by civilian employees of the United States Government, an agency may store the executed copy of the SF 312 and SF 189 in the United States Office of Personnel Management's Official Personnel Folder (OPF) as a long-term (right side) document for that employee. 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 original or legally enforceable facsimile of the executed SF 312, SF 189 or SF 189-A of that employee to the Government agency primarily responsible for his or her classified work. A contractor, licensee or grantee of an agency participating in the Defense Industrial Security Program shall deliver the copy or legally enforceable facsimile of the executed SF 312, SF 189 or SF 189-A of a terminated employee to the Defense Industrial Security Clearance Office. Each agency shall inform ISOO of the file systems that it uses to store these agreements for each category of affected individuals.

(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.

[53 FR 38279, Sept. 29, 1988, as amended at 56 FR 2645, Jan. 23, 1991; 56 FR 27559, June 14, 1991]

QUESTIONS AND ANSWERS

This section includes a series of questions and answers that relate to the background and implementation of the SF 312.

Question 1: What is the Information Security Oversight Office?

Answer: Under Executive Order 12958, "Classified National Security Information," the Information Security Oversight Office (ISOO) is responsible for monitoring the security classification 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 12958, 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.. 12958 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: Executive Order 12958 dated April 17, 1995, requires that a person may have access to classified information provided that person meets three requirements, one of which is signing an approved nondisclosure agreement. National Security Decision Directive No. 84, dated March 11, 1983, also provides that: "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 preconditions: (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 non-disclosure 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 and executive order, the execution of an approved nondisclosure agreement shall be a condition of access 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 she 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 and the 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 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 1.2 and 1.4(e) of Executive Order 12958 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 12958, "Classified 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 agency or a non-Government employee whose clearance is granted through that agency.

An authorized representative of a contractor, licensee, grantee, or other 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. sec. 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 12958, Sec. 1.8(a), specifically prohibits classification "in order to: (1) conceal violations of law, inefficiency, or administrative error; (2) to prevent embarrassment to a person, organization, or agency; (3) to restrain competition; or (4) 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 must establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures must ensure that: (1) individuals are not subject to retribution for bringing such actions; (2) an opportunity is provided for review by an impartial official or panel; and (3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of Executive Order 12958.

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, such as computer disks or electronic storage media, 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. For agreements executed by civilian employees of the United States Government, an agency may store the executed copy of the SF 312 and the SF 189 in the United States Office of Personnel Management's Official Personnel Folder(OPF) as a long-term (right side) document for that employee.

An agency may permit its contractors, licensees and grantees to retain the executed agreements of their employees during the time of employment. Upon termination of employment, the contractor, licensee or grantee shall deliver the original or legally enforceable facsimile of the executed SF 312, SF 189 or SF 189-A of that employee to the Government agency primarily responsible for his or her classified work. A contractor, licensee or grantee of an agency participating in the National Industrial Security Program, for which the Department of Defense is acting as the Cognizant Security Agency, shall deliver the copy of the legally enforceable facsimile of the executed SF 312, SF 189 or SF 189-A of a terminated employee to the Defense Industrial Security Clearance Office.

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.

Question 23: Are Restricted Data and Formerly Restricted Data, classified under the Atomic Energy Act of 1954, as amended, included in the definition for "classified information," as used in the SF 312?

Answer: Yes.

References

Information Security Oversight Office. (2016, August 15). Standard Form 312. Retrieved April 3, 2019, from https://www.archives.gov/isoo/training/standard-form-312.html