Classified Information Nondisclosure Agreement
(Standard Form 312)
Briefing Booklet

Reviewed August 2016

Title 18, United States Code

Sec. 793. Gathering, transmitting or losing defense information

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;

(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

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

EXTRATERRITORIAL JURISDICTION

(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

(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

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

the answer is no. However, if the location and retrieval of a previously signed

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

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

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

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.

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.