

Originally Processed With FOIA(s):
2019-1493-S

FOIA Number:
2019-1493-S

FOIA MARKER

**This is not a textual record. This is used as an
administrative marker by the George Bush Presidential
Library Staff.**

Record Group/Collection: George H.W. Bush Presidential Records
Collection/Office of Origin: National Security Council
Series: H-Files
Subseries: IF Transition Files

OA/ID Number: 99017
Folder ID Number: 99017-002

Folder Title:
NSC Procedural Manual - Binder 1 [2]

Stack:	Row:	Section:	Shelf:	Position:
V	0	0	0	0

Withdrawal/Redaction Sheet (George Bush Library)

Doc. No. / Type	Subject/Title	Date	Restriction	Classification
01. Memorandum	For James McCue Re: Clarification of Nondisclosure Agreements (1 pp.)	9/26/88	(b)(1)	
02. Memorandum	For Paul Schott Stevens From: ISOO Re: Request for visit approval (1 pp.)	6/13/88	(b)(6)	

Page 1 of 1

Collection:

Record Group: Bush Presidential Records
Office: National Security Council
Series: H-Files
Subseries: Transition Files
WHORM Cat.:
File Location: NSC Procedural Manual - Binder 1 [2]

Pinksheet Number: MB14495
OA/ID Number: 99017-002
Date Closed: 9/4/2019
FOIA/Sys Case #: 2019-1493-S
Re-review Case #:
P-2/P-5 Review Case #:

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

December 8, 1988

MEMORANDUM FOR NSC STAFF

FROM: DIRECTOR, NSC SECURITY PROGRAMS *JM*

SUBJECT: Protection of Classified Material

One of the hazards of protecting classified information occurs when personnel with authorized access to highly sensitive information become less security conscious than they should be.

Within the past five months we have had two lapses of security involving highly sensitive national security information. In both instances, a classified document was left unattended in a public area.

It is the responsibility of every member of the NSC to recognize their responsibility for ensuring that classified material is properly protected. Classified material is to be read only in an approved area. If there is a need to stop at a non-secure room or public area, while in possession of a classified document, make certain you keep it in your possession at all times and have it with you when you leave the room or area.

Your attention to this matter is imperative, especially since there are a large number of public rooms to which both cleared and uncleared personnel, including visitors, tour groups, and others, have access.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

October 12, 1988

ACTION

MEMORANDUM FOR PAUL SCHOTT STEVENS

FROM: NICHOLAS ROSTOW *NR*.

SUBJECT: Notice of Clarifications to Classified
Nondisclosure Agreements

Pursuant to a recent order of the United States District Court for the District of Columbia, the Information Security Oversight Office has issued a clarification of every signed copy of the standard classified information nondisclosure agreement (Tab III) and the Director of Central Intelligence has issued a similar clarification of every signed Sensitive Compartmented Information nondisclosure agreement containing the word "classifiable" (Tab IV).

In order to comply with the court order, the National Security Council must notify all persons who were employees (including consultants) on September 25, 1988, who have executed nondisclosure agreements containing the word "classifiable," of the clarifications by October 26.

Based on the records maintained by the Office of Security, we have prepared the memorandum at Tab I to notify NSC employees who have signed the standard nondisclosure agreement and the memorandum at Tab II to notify NSC employees who have signed the SCI nondisclosure agreement.

Jim McCue, *Nancy Menan*, *Brian Merchant* and *George Van Eron*
concur.

RECOMMENDATION

That you sign the two attached memoranda.

Approve _____

Disapprove _____

Attachments

- Tab I - Standard Nondisclosure Agreement Memorandum and distribution list
- Tab II - SCI Nondisclosure Agreement Memorandum and distribution list
- Tab III - Garfinkel Memorandum to Stevens, dated September 29, 1988
- Tab IV - Moroney Memorandum to McCue, dated September 26, 1988

TAB

I

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

ACTION

MEMORANDUM FOR NSC STAFF, NSC CONSULTANTS

FROM: PAUL SCHOTT STEVENS
SUBJECT: Standard Nondisclosure Agreement

As a condition of access to classified information, you have been asked to sign one or more classified information nondisclosure agreements. When you began work as staff members to the National Security Council (prior to January 1988), you were asked to sign Standard Form 189, a standard nondisclosure agreement.

Pursuant to a recent order of the United States District Court for the District of Columbia and as the attached notice (two copies) states, every executed copy of Standard Form 189, "Classified Information Nondisclosure Agreement," is clarified by a rule issued by the Information Security Oversight Office (ISOO).

To indicate that you have received the attached notice, please sign and date one copy of the attached notice and return it by October 17, 1988, to:

James T. McCue
Director, NSC Security Programs
Rm. 401, OEOB

The second copy of the notice is for your records.

ISOO has issued a new nondisclosure agreement, SF 312. Because you have previously signed the SF 189, you need not execute the new nondisclosure form. At your discretion, however, you may elect to substitute a signed copy of the new nondisclosure form, SF 312, for a previously signed SF 189. If you select this option, please contact James McCue at x6130. If you need further information, please contact Robin Frank at x5026.

Attachments

DISTRIBUTION

Scot Addis
Florence Bagnall
Marybel Batjer
Patricia Battenfield
Ralph Bellamy
Stephen E. Benko
William Blitgen
Richard E. Boehlein
Charlene Bolinski
Linton Brooks
Barbara Browne
Susan G. Bunch
William J. Burns
B. J. Burson
Linda Crowell
Charles Wade Chambers
Lance W. Charnes
Richard T. Childress
Peter J. Christensen
William Clark
Maria D. Clark
Theresa A. Clark
Tyrus Cobb
Herman J. Cohen
Mary Cooper
Patricia Corcoran
Anita Craig
Joanne E. Curtiss
Stephen Danzansky
James W. Davis
Roger G. DeKok
Barbara A. Desina
Arlene Dona
Michael B. Donley
Stephen Farrar
Chris T. Featherstone
John W. Ficklin
Entell Ford
Alison Fortier
Florence Gantt
Kathy Gibbs
Wilma G. Hall
George William Heiser
Mary Henhoefffer
Jeanne Hickie
Brenda Hilliard
Baerbel K. Houck
Jeffrey L. Hughes
Lois A. Jago
Lisa Jameson

Janet M. Jeffers
Thelma Peggy Jordan
Gilda Kay
David Barry Kelly
James A. Kelly
Sandra A. Kelly
Barry P. Kiernan
Michael C. Kimberling
James W. Koehler
Gary Langlie
M. Kay LaPlante
Paul J. Lebras
Nelson C. Ledsky
John F. Lewis
Robert E. Linhard
Pamela Loew
Julie Madison Porta
Donald A. Mahley
Betty Marshall
Andre McGuire
Eric Melby
Nancy V. Menan
Brian Merchant
Cathy L. Millison
James F. Miskel
Elaine Mitsler
Angelyn D. Moody
Gary L. Moore
Mark Morrison
Jacqueline Murphy
M. Elise Neil
Rita P O'Flinn
Douglas H. Paal
Helen Pahlke
Flora B. Paoli
Robert Pastorino
Beverly L. Petchel
Alan Peterson
Colin L. Powell
Arthur L. Pridemore
Dona S. Proctor
Karen Prokop
James F. Purdon
Jeffrey T. Rathbun
Patricia A. Rawson
Joan Ritter
Peter Rodman
Diane Ross
Nicholas Rostow
Richard M. Saunders
Norma Schillaci
Marilyn Shapiro
Ralph H. Sigler
Donna M. Sirko

Helen Skaltsounis
Don M. Snider
Daniel L. Snyder
Steven Steiner
Paul S. Stevens
Mary Kay Stults
Shirin Tahir-Kheli
Don Tice
William Tobey
Joan R. Vail
George Van Eron
Bill Van Horn
Sandra Wiley
Bret Wilson
Dolores Wilson
Kay Zerwick
Charles Zingler

NOTICE

TO ALL PERSONS WHO HAVE SIGNED THE STANDARD FORM 189
"CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT"
OR THE STANDARD FORM 189-A
"CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT
(INDUSTRIAL/COMMERCIAL/NON-GOVERNMENT)"

1. By a rule issued by the Information Security Oversight Office, published in the Federal Register on September 29, 1988, implementing an order of the United States District Court for the District of Columbia, the second sentence of Paragraph 1 of every executed copy of the Standard Form 189, "Classified Information Nondisclosure Agreement," 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. The Information Security Oversight Office has issued a new "Classified Information Nondisclosure Agreement," Standard Form 312, to be executed by all cleared Government and non-Government employees as a condition of access to classified information. The SF 312 will be used in lieu of the Standard Form 189, "Classified Information Nondisclosure Agreement," and the Standard Form 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 employee who has previously signed the SF 189 or the SF 189-A does not need to execute the SF 312. However, at that employee's discretion, he or she may elect to substitute a signed SF 312 for a previously signed SF 189 or SF 189-A.

3. Scope of "classified information": As used in the SF 312, the SF 189, and the SF 189-A, "classified information" includes 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.

4. 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: (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.

Signature _____
Name (Print) _____
Date _____

NOTICE

TO ALL PERSONS WHO HAVE SIGNED THE STANDARD FORM 189
"CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT"
OR THE STANDARD FORM 189-A
"CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT
(INDUSTRIAL/COMMERCIAL/NON-GOVERNMENT)"

1. By a rule issued by the Information Security Oversight Office, published in the Federal Register on September 29, 1988, implementing an order of the United States District Court for the District of Columbia, the second sentence of Paragraph 1 of every executed copy of the Standard Form 189, "Classified Information Nondisclosure Agreement," 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. The Information Security Oversight Office has issued a new "Classified Information Nondisclosure Agreement," Standard Form 312, to be executed by all cleared Government and non-Government employees as a condition of access to classified information. The SF 312 will be used in lieu of the Standard Form 189, "Classified Information Nondisclosure Agreement," and the Standard Form 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 employee who has previously signed the SF 189 or the SF 189-A does not need to execute the SF 312. However, at that employee's discretion, he or she may elect to substitute a signed SF 312 for a previously signed SF 189 or SF 189-A.

3. Scope of "classified information": As used in the SF 312, the SF 189, and the SF 189-A, "classified information" includes 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.

4. 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: (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.

TAB

II

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

ACTION

MEMORANDUM FOR NSC STAFF, NSC CONSULTANTS

FROM: PAUL SCHOTT STEVENS

SUBJECT: Sensitive Compartmented Information Nondisclosure Agreement

As a condition of access to information or material protected within Special Access Programs, you were asked to sign a Sensitive Compartmented Information Nondisclosure Agreement, either Standard Form 4193 or an equivalent agreement, when you began working at the NSC.

Pursuant to a recent order of the United States District Court for the District of Columbia, the language of Standard Form 4193 and equivalent nondisclosure agreements is clarified, as the attached notice (two copies) indicates.

To indicate that you have received the attached notice, please sign and date one copy and return it by October 17, 1988, to:

James T. McCue
Director, NSC Security Programs
Rm. 401, OEOB

The second copy of the notice is for your records.

The Director of Central Intelligence has issued a new SCI Nondisclosure Agreement, SF 4355. Because you have previously signed the SF 4193 or its equivalent, you need not execute the SF 4355. At your discretion, however, you may elect to substitute a signed copy of the new nondisclosure form, SF 4355, for a previously signed SF 4193. If you select this option, please contact James McCue at x6130. If you need further information, please contact Robin Frank at x5026.

Attachments

DISTRIBUTION

Scot Addis
Florence Bagnall
Marybel Batjer
Patricia Battenfield
Stephen E. Benko
Richard E. Boehlein
Charlene Bolinski
Linton Brooks
Barbara Browne
Susan G. Bunch
William J. Burns
B. J. Burson
Linda Crowell
Charles Wade Chambers
Lance W. Charnes
Peter J. Christensen
William Clark
Maria D. Clark
Theresa Clark
William Cockell
Herman J. Cohen
Mary Cooper
Patricia Corcoran
Joanne E. Curtiss
Michael Daniels
Stephen Danzansky
Eva-Marie Davis
Roger G. DeKok
Mary A Dix
Arlene Dona
Michael B. Donley
Stephen Farrar
Chris T. Featherstone
Entell Ford
Alison Fortier
Christina Funches
Kathy Gibbs
Wendy E. Gray
John G. Grimes
Wilma G. Hall
Dave Hawes
George William Heiser
Mary Henhoeffter
Eric Herbst
Jeanne Hickie
Brenda Hilliard
Baerbel K. Houck
Jeffrey L. Hughes
Lois A. Jago
Janet M. Jeffers
Kenneth Johnson

Thelma Peggy Jordan
Gilda Kay
David Barry Kelly
James A. Kelly
Sandra A. Kelly
Barry P. Kiernan
Michael C. Kimberling
James W. Koehler
Amy Korpeck
Gary Langlie
M. Kay LaPlante
Joseph E. Laposa
Paul J. Lebras
Nelson C. Ledsky
Mary T. Leonard
Daniel Levin
John F. Lewis
Robert E. Linhard
Pamela Loew
Julie Madison Porta
Donald A. Mahley
Betty Marshall
Andre McGuire
Nancy V. Menan
Jeffrey M. Menath
Brian Merchant
Cathy L. Millison
James F. Miskel
Carol D. Mitchell
Elaine Mitsler
Gary L. Moore
Mark Morrison
Jacqueline Murphy
M. Elise Neil
Rita P O'Flinn
Douglas H. Paal
Helen Pahlke
Flora B. Paoli
Carol A. Paquette
Beverly L. Petchel
Alan Peterson
Richard Porter
Colin L. Powell
Arthur L. Pridemore
Dona S. Proctor
Karen Prokop
James F. Purdon
Jeffrey T. Rathbun
Patricia A. Rawson
Joan Ritter
Peter Rodman
Diane Ross
Nicholas Rostow

Richard M. Saunders
Norma Schillaci
Marilyn Shapiro
Ralph H. Sigler
Donna M. Sirko
Helen Skaltsounis
Don M. Snider
Steven Steiner
Paul S. Stevens
Mary Kay Stults
Shirin Tahir-Kheli
Don Tice
Jacqueline Tillman
William Tobey
Joan R. Vail
George Van Eron
Bill Van Horn
Sandra Wiley
Bret Wilson
Dolores Wilson
Julian T. Wolfe
Kay Zerwick
Charles Zingler

CLARIFICATION OF FORM 4193 AND EQUIVALENT
SCI NONDISCLOSURE AGREEMENTS

Please be advised that, in conformance with the order of the United States District Court for the District of Columbia, the following is substituted for the term "classifiable" in all Sensitive Compartmented Information (SCI) nondisclosure agreements containing that term:

". . . information that is unmarked classified information, including oral communications, and unclassified information that meets the standards for classification and is in the process of a classification determination . . ."

By making this substitution, the Director of Central Intelligence is clarifying that SCI nondisclosure agreements that contain the term "classifiable" do not cover currently unclassified information that may be subject to classification at some future date, but is not currently in the process of a classification determination. Therefore, the only circumstances under which a signatory might violate the terms of an SCI nondisclosure agreement by disclosing unclassified information are when a signatory knows, or reasonably should know, that such information is in the process of a classification determination and requires interim protection as provided in section 1.1(c) of Executive Order 12356 or any other statute or Executive order that requires interim protection for certain unclassified information while a classification determination is pending.

Thus, a signatory of an SCI nondisclosure agreement containing the word "classifiable" may be liable for disclosing information falling within the substituted phrase if:

(a) He or she knows that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, whether the unauthorized disclosure is willful or negligent; or

(b) He or she should know that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, in which case the unauthorized disclosure is negligent. In no instance could a signatory be liable for violating nondisclosure

provisions by disclosing unmarked information when, at the time of the disclosure, there was no basis to suggest, other than pure speculation, that the information was classified or in the process of a classification determination.

Through this notice, signatories to SCI nondisclosure agreements that contain the term "classifiable" are advised that their continued access to SCI will be governed by the SCI nondisclosure agreement they signed as it has been amended by this notice, without any further action.

Signature _____
Name (Print) _____
Date _____

CLARIFICATION OF FORM 4193 AND EQUIVALENT
SCI NONDISCLOSURE AGREEMENTS

Please be advised that, in conformance with the order of the United States District Court for the District of Columbia, the following is substituted for the term "classifiable" in all Sensitive Compartmented Information (SCI) nondisclosure agreements containing that term:

". . . information that is unmarked classified information, including oral communications, and unclassified information that meets the standards for classification and is in the process of a classification determination . . ."

By making this substitution, the Director of Central Intelligence is clarifying that SCI nondisclosure agreements that contain the term "classifiable" do not cover currently unclassified information that may be subject to classification at some future date, but is not currently in the process of a classification determination. Therefore, the only circumstances under which a signatory might violate the terms of an SCI nondisclosure agreement by disclosing unclassified information are when a signatory knows, or reasonably should know, that such information is in the process of a classification determination and requires interim protection as provided in section 1.1(c) of Executive Order 12356 or any other statute or Executive order that requires interim protection for certain unclassified information while a classification determination is pending.

Thus, a signatory of an SCI nondisclosure agreement containing the word "classifiable" may be liable for disclosing information falling within the substituted phrase if:

(a) He or she knows that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, whether the unauthorized disclosure is willful or negligent; or

(b) He or she should know that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, in which case the unauthorized disclosure is negligent. In no instance could a signatory be liable for violating nondisclosure

provisions by disclosing unmarked information when, at the time of the disclosure, there was no basis to suggest, other than pure speculation, that the information was classified or in the process of a classification determination.

Through this notice, signatories to SCI nondisclosure agreements that contain the term "classifiable" are advised that their continued access to SCI will be governed by the SCI nondisclosure agreement they signed as it has been amended by this notice, without any further action.

TAB

III



Information Security Oversight Office
Washington, DC 20405



September 29, 1988

Dear Mr. Stevens:

The purpose of this letter is two-fold. First, it announces the issuance by the Information Security Oversight Office (ISOO) of a new "Classified Information Nondisclosure Agreement," the Standard Form 312. Second, it advises you of a clarification to previously executed copies of the Standard Form 189, also entitled "Classified Information Nondisclosure Agreement," and your requirement to communicate this clarification no later than October 27, 1988, to all employees who have previously executed the SF 189.

I. The Standard Form 312

In accordance with National Security Decision Directive 84 (NSDD 84), dated March 11, 1983, ISOO has today issued a rule that implements the Standard Form 312, "Classified Information Nondisclosure Agreement (SF 312). Effective immediately, the SF 312 shall serve as the instrument to fulfill the following requirement found in Paragraph 1(a) of NSDD 84: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access."

On December 29, 1987, ISOO imposed a moratorium on the further execution of nondisclosure agreements issued to implement NSDD 84. With respect to the SF 312, that moratorium is now lifted. Further, on August 21, 1987, ISOO imposed a moratorium on the withdrawal of access and security clearances of persons who are required to execute a nondisclosure agreement as a condition of access to classified information but who refuse to do so. With respect to the required execution of the SF 312, that moratorium also is lifted.

ISOO has issued the SF 312 to replace both the Standard Form 189, "Classified Information Nondisclosure Agreement" (SF 189), and the Standard Form 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)" (SF 189-A). However, executed copies of both the SF 189 and the SF 189-A remain valid, and fulfill that requirement of NSDD 84 quoted above. Therefore, you are required to obtain the execution of SF 312 by only those cleared Government and non-Government employees who have not previously signed either the SF 189 or SF 189-A.

Any person who has executed the SF 189 or SF 189-A may elect, however, to substitute a signed SF 312 for the previously executed agreement. You must take all reasonable steps to notify affected employees of this option, and, when an employee exercises it, to replace the previously signed nondisclosure agreement with the executed SF 312. ISOO strongly suggests the use of the enclosed "Notice to Employees," or a similar notice, for this purpose.

II. Modification of the SF 189

In accordance with a recent ruling of the United States District Court for the District of Columbia, ISOO has included in today's rule a provision that strikes the word "classifiable" from Paragraph 1 of each executed copy of the SF 189, while substituting language that clarifies the scope of "classified information," as used in the agreement. The rule also provides a definition of the scope of the term "classified information" in the SF 312, SF 189 and SF 189-A, and recites the basis for liability for violating any of these agreements. These references assure consistency in the enforcement of any of these agreements that implement NSDD 84.

On Friday, September 23, 1988, the court denied the Government's motion to substitute constructive notice through publication in the Federal Register for personal notice to every affected employee. Under the court's order, the Government must notify every employee who has executed the SF 189 of this clarification no later than October 27, 1988. When logistical circumstances do not permit compliance within that time frame for particular individuals, you should continue with efforts to notify them as quickly as possible. To assist you in meeting this notification requirement, we enclose a copy of a suggested notice, which is based upon the rule issued today. This notice, or one based upon it, may be reproduced in any format, and distributed as required. No actual physical alteration of the executed SF 189s is necessary, nor are agencies required to obtain receipts from employees that they have received notice.

The court order does not require that you notify former employees of this clarification, and, in the interest of seeking the most timely compliance, ISOO is also not imposing this requirement. Even without this notice, copies of the SF 189 executed by former employees will be enforced as the language in Paragraph 1 has been clarified.

ISOO is printing an initial stock of the SF 312 for distribution to the agencies. We will be working with your liaison to ISOO to make these arrangements. You should procure additional copies of the SF 312 through regular supply channels.

We enclose for your information and use a copy of the rule published in the Federal Register today that implements the SF 312, strikes the word "classifiable" and otherwise clarifies Paragraph 1 of the SF 189; ten sample copies of the SF 312; a copy of ISOO's suggested "Notice for Employees," taken from the published rule; and a series of questions and answers that should help answer many of your questions and the questions of employees that will arise regarding the SF 312. We are currently working on the production of a videotape and booklet that should prove to be useful briefing aids on the SF 312. We will notify you when they become available.

Please keep your ISOO liaison informed of the actions taken by your agency to implement the requirements set forth in this letter and rule. For answers to your questions, please contact ISOO at FTS 535-7251, or (202) 535-7251.

Sincerely,


Steven Garfinkel
Director

The Honorable
Paul Schott Stevens
Executive Secretary
National Security Council
The White House
Washington, DC 20500

Enclosures

Final Rule

Thursday
September 29, 1988

Part VI

**Information Security
Oversight Office**

32 CFR Part 2003

**National Security Information; Standard
Forms; Final Rule**

INFORMATION SECURITY OVERSIGHT OFFICE**32 CFR Part 2003****National Security Information; Standard Forms**

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Final rule.

SUMMARY: This amendment to 32 CFR 2003.20 provides for: (1) the issuance and use of Standard Form 312, "Classified Information Nondisclosure Agreement" (SF 312); and (2) the modification of Paragraph 1 of all previously executed copies of Standard Form 189, "Classified Information Nondisclosure Agreement" (SF 189), to strike the word "classifiable" and to substitute in its place language that clarifies the scope of "classified information" as used in those agreements. From the effective date of this rule, the SF 312 shall be used in lieu of its predecessor nondisclosure agreements, SF 189 and Standard Form 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)" (SF 189-A). ISOO is issuing the SF 312 as a preferred means of clarifying the scope of some language in the SF 189 and the SF 189-A that has been at issue in litigation concerning the constitutionality and legality of certain nondisclosure agreements, including the SF 189. Notwithstanding the changes in some of its language, the SF 312 does not in any way differ from its predecessor nondisclosure agreements with respect to the substance of the information that each is intended to protect. ISOO is clarifying executed copies of the SF 189 to comply with a recent order of the United States District Court for the District of Columbia, to take account of statutory provisions that reflect congressional concern regarding possible ambiguity of the word "classifiable," and to make the language of the SF 189 more consistent with the language of the SF 312 and the SF 189-A.

EFFECTIVE DATE: September 29, 1988.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO, 202-535-7251.

SUPPLEMENTARY INFORMATION: This amendment to 32 CFR Part 2003 is issued pursuant to section 5.2(b)(7) of Executive Order 12356, "National Security Information," which grants the Director of ISOO the authority to issue standardized security forms, and Paragraph 1 of National Security Decision Directive 84, March 11, 1983,

which directs ISOO to issue a standardized nondisclosure agreement to be signed as a condition of access by all persons cleared for access to classified information. In fulfilling this requirement, ISOO has previously issued two nondisclosure agreements: SF 189, "Classified Information Nondisclosure Agreement," in September 1983; and SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)," in November 1986.

On December 29, 1987, ISOO directed agencies to halt further implementation of the SF 189 and SF 189-A as a result of the enactment of section 630 of the Treasury, Postal Service, and General Appropriations Act, 1988, which was part of the Omnibus Continuing Resolution for Fiscal Year 1988 (Pub. L. 100-202). On May 27, 1988, in litigation primarily involving the constitutionality and legality of the SF 189, the United States District Court for the District of Columbia ruled that Section 630 of Public Law 100-202 is unconstitutional (*National Federation of Federal Employees v. United States, et al.*, Civil Action No. 87-2284-OG; *American Federation of Government Employees, et al. v. Garfinkel, et al.*, Civil Action No. 87-2412-OG; *American Foreign Service Association, et al. v. Garfinkel, et al.*, Civil Action No. 88-0440-OG). In a subsequent ruling of July 28, 1988, in the first two of the above-captioned cases, the same court upheld the constitutionality and legality of the SF 189. However, the court also ruled that in order to bring the scope of the word "classifiable" within constitutional limits, the SF 189 must be modified, either (a) by providing each signatory a copy of ISOO's definition of "classifiable information," as published in 52 FR 48367 on December 21, 1987; or (b) by striking the word from executed copies of the agreement. Notwithstanding these rulings upholding the validity of the predecessor nondisclosure agreements, ISOO has concluded that, in lifting the moratorium on the execution of required nondisclosure agreements, a preferred means to deal with the perceived ambiguities in their language is the issuance of a new nondisclosure agreement, the SF 312. The SF 312 avoids as many of these perceived problem areas as possible without changing the substance of the classified information that the nondisclosure agreement is intended to protect. In issuing the SF 312, ISOO does not seek its execution by every cleared Government or industry employee who has already executed an SF 189 or an SF 189-A, since these total over two million

individuals. However, the rule provides that every individual who previously signed an SF 189 or SF 189-A may substitute a signed copy of the SF 312 at his or her own choosing. Also, through this rule ISOO is instructing agencies to enforce the predecessor agreements in a manner that is fully consistent with the enforcement of the SF 312. To help achieve greater consistency, ISOO is complying with the court order by opting to strike the word "classifiable" from the SF 189, while substituting language that clarifies the scope of "classified information," as used in the agreement. This language is taken from the definition of "classifiable" previously published in the Code of Federal Regulations, and adjudged by the District Court to bring the definition within constitutional and legal standards. ISOO has not included the word "classifiable" in the SF 312, and did not previously include it in the SF 189-A, although these agreements are both intended to protect the same information protected by the SF 189. The word "classifiable" had been included in the SF 189 not to introduce concepts separate and distinct from classified information, but to emphasize the need to protect unmarked classified information and information in the process of a classification determination. Therefore, striking the word from the SF 189 is the more consistent of the two options presented by the court, while its concepts remain protected within the scope of classified information.

Concurrent with the issuance of the SF 312, by a letter of this date the ISOO Director is instructing the senior official for information security oversight in each agency that creates or handles classified information to lift the current moratorium on the execution of the "Classified Information Nondisclosure Agreement," imposed by letter of December 29, 1987; and to lift the moratorium on the withdrawal of access to classified information and security clearances, imposed by letter of August 21, 1987, for those cleared persons who refuse to sign the SF 312.

Before issuing the SF 312, ISOO submitted drafts for review and comment to the executive branch agencies most affected by it; to seven Committees or Subcommittees of the Congress most involved with the subject of classified information; and to selected interest groups actively concerned with this subject. ISOO has considered those comments that it has received in response to its solicitations, and, when ISOO concluded that suggested changes were warranted, it has incorporated

INFORMATION SECURITY OVERSIGHT OFFICE**32 CFR Part 2003****National Security Information; Standard Forms**

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Final rule.

SUMMARY: This amendment to 32 CFR 2003.20 provides for: (1) the issuance and use of Standard Form 312, "Classified Information Nondisclosure Agreement" (SF 312); and (2) the modification of Paragraph 1 of all previously executed copies of Standard Form 189, "Classified Information Nondisclosure Agreement" (SF 189), to strike the word "classifiable" and to substitute in its place language that clarifies the scope of "classified information" as used in those agreements. From the effective date of this rule, the SF 312 shall be used in lieu of its predecessor nondisclosure agreements, SF 189 and Standard Form 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)" (SF 189-A). ISOO is issuing the SF 312 as a preferred means of clarifying the scope of some language in the SF 189 and the SF 189-A that has been at issue in litigation concerning the constitutionality and legality of certain nondisclosure agreements, including the SF 189. Notwithstanding the changes in some of its language, the SF 312 does not in any way differ from its predecessor nondisclosure agreements with respect to the substance of the information that each is intended to protect. ISOO is clarifying executed copies of the SF 189 to comply with a recent order of the United States District Court for the District of Columbia, to take account of statutory provisions that reflect congressional concern regarding possible ambiguity of the word "classifiable," and to make the language of the SF 189 more consistent with the language of the SF 312 and the SF 189-A.

EFFECTIVE DATE: September 29, 1988.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO, 202-535-7251.

SUPPLEMENTARY INFORMATION: This amendment to 32 CFR Part 2003 is issued pursuant to section 5.2(b)(7) of Executive Order 12356, "National Security Information," which grants the Director of ISOO the authority to issue standardized security forms, and Paragraph 1 of National Security Decision Directive 84, March 11, 1983,

which directs ISOO to issue a standardized nondisclosure agreement to be signed as a condition of access by all persons cleared for access to classified information. In fulfilling this requirement, ISOO has previously issued two nondisclosure agreements: SF 189, "Classified Information Nondisclosure Agreement," in September 1983; and SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)," in November 1986.

On December 29, 1987, ISOO directed agencies to halt further implementation of the SF 189 and SF 189-A as a result of the enactment of section 630 of the Treasury, Postal Service, and General Appropriations Act, 1988, which was part of the Omnibus Continuing Resolution for Fiscal Year 1988 (Pub. L. 100-202). On May 27, 1988, in litigation primarily involving the constitutionality and legality of the SF 189, the United States District Court for the District of Columbia ruled that Section 630 of Public Law 100-202 is unconstitutional (*National Federation of Federal Employees v. United States, et al.*, Civil Action No. 87-2284-OG; *American Federation of Government Employees, et al. v. Garfinkel, et al.*, Civil Action No. 87-2412-OG; *American Foreign Service Association, et al. v. Garfinkel, et al.*, Civil Action No. 88-0440-OG). In a subsequent ruling of July 28, 1988, in the first two of the above-captioned cases, the same court upheld the constitutionality and legality of the SF 189. However, the court also ruled that in order to bring the scope of the word "classifiable" within constitutional limits, the SF 189 must be modified, either (a) by providing each signatory a copy of ISOO's definition of "classifiable information," as published in 52 FR 48367 on December 21, 1987; or (b) by striking the word from executed copies of the agreement.

Notwithstanding these rulings upholding the validity of the predecessor nondisclosure agreements, ISOO has concluded that, in lifting the moratorium on the execution of required nondisclosure agreements, a preferred means to deal with the perceived ambiguities in their language is the issuance of a new nondisclosure agreement, the SF 312. The SF 312 avoids as many of these perceived problem areas as possible without changing the substance of the classified information that the nondisclosure agreement is intended to protect. In issuing the SF 312, ISOO does not seek its execution by every cleared Government or industry employee who has already executed an SF 189 or an SF 189-A, since these total over two million

individuals. However, the rule provides that every individual who previously signed an SF 189 or SF 189-A may substitute a signed copy of the SF 312 at his or her own choosing. Also, through this rule ISOO is instructing agencies to enforce the predecessor agreements in a manner that is fully consistent with the enforcement of the SF 312. To help achieve greater consistency, ISOO is complying with the court order by opting to strike the word "classifiable" from the SF 189, while substituting language that clarifies the scope of "classified information," as used in the agreement. This language is taken from the definition of "classifiable" previously published in the Code of Federal Regulations, and adjudged by the District Court to bring the definition within constitutional and legal standards. ISOO has not included the word "classifiable" in the SF 312, and did not previously include it in the SF 189-A, although these agreements are both intended to protect the same information protected by the SF 189. The word "classifiable" had been included in the SF 189 not to introduce concepts separate and distinct from classified information, but to emphasize the need to protect unmarked classified information and information in the process of a classification determination. Therefore, striking the word from the SF 189 is the more consistent of the two options presented by the court, while its concepts remain protected within the scope of classified information.

Concurrent with the issuance of the SF 312, by a letter of this date the ISOO Director is instructing the senior official for information security oversight in each agency that creates or handles classified information to lift the current moratorium on the execution of the "Classified Information Nondisclosure Agreement," imposed by letter of December 29, 1987; and to lift the moratorium on the withdrawal of access to classified information and security clearances, imposed by letter of August 21, 1987, for those cleared persons who refuse to sign the SF 312.

Before issuing the SF 312, ISOO submitted drafts for review and comment to the executive branch agencies most affected by it; to seven Committees or Subcommittees of the Congress most involved with the subject of classified information; and to selected interest groups actively concerned with this subject. ISOO has considered those comments that it has received in response to its solicitations, and, when ISOO concluded that suggested changes were warranted, it has incorporated

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.

Dated: September 23, 1988.

Steven Garfinkel,

Director, Information Security Oversight Office.

[FR Doc. 88-22232 Filed 9-26-88; 8:45 am]

BILLING CODE 6820-KC-M



Information Security Oversight Office
Washington, DC 20405



STANDARD FORM 312
CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

QUESTION	PAGE NO.
WHAT IS THE INFORMATION SECURITY OVERSIGHT OFFICE (ISOO)?.....	3
WHAT IS THE PURPOSE OF A NONDISCLOSURE AGREEMENT?.....	3
UPON WHAT LEGAL AUTHORITY IS THE SF 312 BASED?.....	4
WHO MUST SIGN THE SF 312?.....	4
ARE ALL MEMBERS OF CONGRESS, AS CONSTITUTIONALLY ELECTED OFFICE-HOLDERS, ENTITLED TO UNLIMITED ACCESS TO CLASSIFIED INFORMATION?.....	5
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?.....	5
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?.....	6
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?.....	6
HOW MUCH TIME SHOULD AN AGENCY OR CONTRACTOR PROVIDE AN EMPLOYEE TO DECIDE WHETHER TO SIGN THE SF 312?.....	7
WHAT STEPS SHOULD BE TAKEN IF A PERSON WHO HAS NOT SIGNED EITHER THE SF 189 OR SF 189-A REFUSES TO SIGN THE SF 312?.....	8
HOW DOES THE SF 312 DIFFER FROM THE SF 189 AND SF 189-A?.....	9
FOR PURPOSES OF THE SF 312, WHAT IS "CLASSIFIED INFORMATION"?.....	10
WHAT IS THE THRESHOLD FOR LIABILITY FOR VIOLATING THE NONDISCLOSURE PROVISIONS OF THE SF 312?.....	10

WHY WAS THE TERM "CLASSIFIABLE" NOT INCLUDED IN THE SF 312?.....	11
MAY THE LANGUAGE OF THE SF 312 BE ALTERED TO SUIT THE PREFERENCES OF AN INDIVIDUAL SIGNER?.....	11
DOES THE SF 312 CONFLICT WITH THE "WHISTLEBLOWER" STATUTE?.....	12
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?.....	12
HOW LONG DO AGENCIES AND CONTRACTORS HAVE TO FULFILL THE REQUIREMENT TO IMPLEMENT THE EXECUTION OF THE SF 312 BY CLEARED EMPLOYEES?.....	13
WHAT KIND OF BRIEFING OR OTHER INFORMATION SHOULD AN AGENCY OFFER AT THE TIME A PERSON IS ASKED TO SIGN THE SF 312?.....	14
IF A PERSON WHO HAS PREVIOUSLY SIGNED THE SF 189 OR SF 189-A OPTS TO SIGN AND SUBSTITUTE THE SF 312, MUST HE OR SHE ALSO RECEIVE ANOTHER BRIEFING?.....	14
WHAT STEPS MUST AN AGENCY OR CONTRACTOR TAKE TO SUBSTITUTE A SIGNED SF 312 FOR A SIGNED SF 189 OR SF 189-A? IF REQUESTED, MUST THE AGENCY OR CONTRACTOR RETURN THE PREVIOUSLY SIGNED FORM TO THE SIGNATORY?.....	15
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?.....	15
MAY THE SIGNER KEEP A COPY OF THE EXECUTED SF 312?.....	16

Q: What is the Information Security Oversight Office?

A: The Information Security Oversight Office (ISOO), established by Executive Order 12065 (December 1, 1978) and continued under Executive Order 12356 (April 6, 1982), 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.

Q: What is the purpose of a nondisclosure agreement?

A: The primary purpose of a nondisclosure agreement 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 unauthorized disclosures or to discipline employees responsible for such disclosures by initiating a civil or administrative action.

Q: Upon what legal authority is the SF 312 based?

A: 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.

Q: Who must sign the SF 312?

A: 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.

Q: Are all Members of Congress, as constitutionally elected office-holders, entitled to unlimited access to classified information?

A: 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.

Q: 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?

A: 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.

Q: 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?

A: 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.

Q: 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?

A: Since every cleared person must sign a nondisclosure agreement, the routine answer to this question is "yes." However, in implementing this program, ISOO has learned of a number of cleared employees who questioned executing a nondisclosure agreement on the basis that they had 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. In these situations, the agency or contractor must be prepared to justify the need for the clearance, since the affected employee may continue to resist executing the SF 312 on the basis that he or she has not had access to classified information.

Q: How much time should an agency or contractor provide an employee to decide whether to sign the SF 312?

A: In all situations, the answer to this question should be governed by what is reasonable under the circumstances. The following examples are illustrative. Because examples such as these and others may result in adversarial proceedings, written documentation of the transaction between the agency/contractor and the employee is critical. Also, in any situation in which there is a delay in the execution of the SF 312, the employee should be briefed on the criminal, civil or administrative consequences that may result from the unauthorized disclosure of classified information, even though the individual has not signed a nondisclosure agreement.

Example I: An employee declares explicitly that under no circumstances will he or she execute the SF 312. He or she should be advised again of the consequences of that decision. If he or she maintains the same position, the agency or contractor should take immediate steps to deny further access to classified information and to initiate the revocation of the clearance.

Example II: An employee requests additional time to consider his or her decision. He or she should be afforded a reasonable period of time to do so. If the requested additional time is 15 days or less, the agency or contractor should ordinarily grant it and make a written record of the established deadline. If the requested period of time is greater than 15 days, what that period of time will be should be discussed between the agency/contractor and employee, and a decision made, recorded, and communicated to the employee before the time begins.

Example III: An employee requests an opportunity to consult with outside counsel. He or she should be afforded a reasonable period of time in which to do so. What that period of time will be should be discussed between the agency/contractor and employee, and a decision made, recorded, and communicated to the employee before the time begins.

Example IV: An employee submits questions about the SF 312, which are reasonable both in number and in content, and requests written answers. He or she should be given a reasonable time to review those answers before any action adverse to the employee is undertaken. If the requested additional time after receipt of the answers is 15 days or less, the agency or contractor should ordinarily grant it and make a written record of the established deadline. If the requested period of time is greater than 15 days, what that period of time will be should be discussed between the agency/contractor and employee, and a decision made, recorded, and communicated to the employee before the time begins.

Q: What steps should be taken if a person who has not signed either the SF 189 or SF 189-A refuses to sign the SF 312?

A: 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.

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

A: 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.

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

A: 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.

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

A: 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.

Q: Why was the term "classifiable" not included in the SF 312?

A: The term "classifiable," as originally used in Paragraph 1 of the SF 189, was not included in the SF 312 to avoid the confusion that arose over the intended scope of that word. The "able" suffix in the word "classifiable" promoted the incorrect interpretation that the word referred to unclassified information that might be classified in the future. Rather, the term "classifiable information" was intended and defined to encompass two narrow classes of information that must be protected under Executive Order 12356, "National Security Information." These are (a) unmarked classified information, including oral communications; and (b) unclassified information that meets the standards for classification and is in the process of a classification determination. In response to a recent order of the United States District Court for the District of Columbia, the word "classifiable" has now been struck from the SF 189 and replaced with language consistent with its previously published definition. The same language is included in the SF 312. Further, in accordance with a rule issued by the Information Security Oversight Office, the SF 189 and the SF 189-A shall be interpreted and enforced in a manner that is fully consistent with the interpretation and enforcement of the SF 312.

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

A: 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.

Q: Does the SF 312 conflict with the "whistleblower" statute?

A: The SF 312 does not conflict with the "whistleblower" statute (5 U.S.C. § 2302). The statute does not extend its protection to 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 employees 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.

Q: 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?

A: 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.

Q: How long do agencies and contractors have to fulfill the requirement to implement the execution of the SF 312 by cleared employees?

A: In issuing the SF 312, ISOO is not establishing at this time a firm deadline for full agency and contractor compliance. However, ISOO encourages agencies that are responsible for Government and non-Government compliance to impose deadlines consistent with logistical realities. ISOO will continue to monitor agency compliance to help ensure that full implementation is achieved in a timely manner.

Further, it should be noted that the effort to achieve full compliance within Government agencies should not be particularly burdensome. At the time ISOO imposed a moratorium on the execution of further copies of the SF 189 at the end of 1987, agencies had reported compliance that approximated 98-99% of the persons required to execute the nondisclosure agreement. To achieve full compliance within Government agencies will require the execution of the SF 312 by the remaining one or two percent of employees; by those employees who have been cleared for access to classified information since the imposition of the moratorium; and by newly cleared employees.

ISOO does not have comparable data for the degree of compliance within industry at the time of the imposition of the moratorium. The Defense Investigative Service and other agencies that are responsible for the security administration of classified contracts, licenses and grants should establish deadlines for full compliance.

Q: What kind of briefing or other information should an agency offer at the time a person is asked to sign the SF 312?

A: At the time an employee is asked to sign the SF 312, the agency or contractor should provide a briefing that, at a minimum, provides information about: (a) the purposes of the nondisclosure agreement; (b) the intent and scope of its provisions; (c) the consequences that will result from the employee's failure to sign the agreement; and (d) the consequences that may result from the unauthorized disclosure of classified information, including possible administrative, civil, or criminal sanctions. In this context, the briefing should explain clearly the procedures to be followed in ascertaining whether a prospective recipient may have access to classified information.

The briefing may be limited to the subject of the SF 312, or it may be in the context of an initial or refresher briefing about the information security system, generally. While the heart of the briefing may be based upon a prepared text or audiovisual, the agency or contractor representative should answer any reasonable questions or concerns raised by the individual regarding the SF 312, or be prepared to obtain answers to those questions. The representative must also have available copies of every statute, executive order or regulation that is referenced in Paragraph 10 of the SF 312.

Q: If a person who has previously signed the SF 189 or SF 189-A opts to sign and substitute the SF 312, must he or she also receive another briefing?

A: The agency or contractor is not required to provide an additional briefing upon execution of the SF 312 in these circumstances. However, the agency or contractor representative should answer any reasonable questions or concerns raised by the individual regarding the SF 312, or be prepared to obtain answers to those questions. The representative should also have available copies of every statute, executive order or regulation that is referenced in Paragraph 10 of the SF 312.

Q: What steps must an agency or contractor take to substitute a signed SF 312 for a signed SF 189 or SF 189-A? If requested, must the agency or contractor return the previously signed form to the signatory?

A: In the event that a signatory opts to substitute a signed SF 312 for a previously signed SF 189 or SF 189-A, the agency or contractor shall dispose of the SF 189 or SF 189-A, either through its physical destruction or, if requested, through its return to the signatory, if these means of disposal can be accomplished with a reasonable amount of effort or expenditure of resources. In situations in which physical disposal is not a reasonable alternative, the agency or contractor shall take all reasonable steps to annotate the retained version of the SF 189 or SF 189-A with markings that make clear that it has been voided; and provide the signatory with an official written statement to that effect. In extraordinary circumstances in which none of the alternatives above is reasonable, the agency or contractor shall provide the signatory with an official written statement that the retained SF 189 or SF 189-A is void. In any circumstances, the SF 189 or SF 189-A should not be destroyed or voided until after the employee has executed the SF 312.

Q: 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?

A: The originals or legally enforceable facsimiles of 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.

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

A: 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.

NOTICE

**TO ALL PERSONS WHO HAVE SIGNED THE STANDARD FORM 189
"CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT"
OR THE STANDARD FORM 189-A
"CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT
(INDUSTRIAL/COMMERCIAL/NON-GOVERNMENT)"**

1. By a rule issued by the Information Security Oversight Office, published in the Federal Register on September 29, 1988, implementing an order of the United States District Court for the District of Columbia, the second sentence of Paragraph 1 of every executed copy of the Standard Form 189, "Classified Information Nondisclosure Agreement," 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. The Information Security Oversight Office has issued a new "Classified Information Nondisclosure Agreement," Standard Form 312, to be executed by all cleared Government and non-Government employees as a condition of access to classified information. The SF 312 will be used in lieu of the Standard Form 189, "Classified Information Nondisclosure Agreement," and the Standard Form 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 employee who has previously signed the SF 189 or the SF 189-A does not need to execute the SF 312. However, at that employee's discretion, he or she may elect to substitute a signed SF 312 for a previously signed SF 189 or SF 189-A.

3. Scope of "classified information": As used in the SF 312, the SF 189, and the SF 189-A, "classified information" includes 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.

4. 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: (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.

5. For further information, please contact:

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Printed or typed)

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)

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 read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
-----------	------	---

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)
(Type or print)

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.

TAB

IV

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
01. Memorandum	For James McCue Re: Clarification of Nondisclosure Agreements (1 pp.)	9/26/88	(b)(1)	

Collection:

Record Group: Bush Presidential Records
Office: National Security Council
Series: H-Files
Subseries: Transition Files
WHORM Cat.:
File Location: NSC Procedural Manual - Binder 1 [2]

Date Closed: 9/4/2019	OA/ID Number: 99017-002
FOIA/SYS Case #: 2019-1493-S	Appeal Case #:
Re-review Case #:	Appeal Disposition:
P-2/P-5 Review Case #:	Disposition Date:
AR Case #:	MR Case #:
AR Disposition:	MR Disposition:
AR Disposition Date:	MR Disposition Date:

RESTRICTION CODES

Freedom of Information Act (FOIA) - [5 U.S.C. 552(b)]

(b)(1) National security classified information
(b)(2) Release would disclose internal personnel rules and practices of an agency
(b)(3) Release would violate a Federal statute
(b)(4) Release would disclose trade secrets or confidential or financial information
(b)(6) Release would constitute a clearly unwarranted invasion of personal privacy
(b)(7) Release would disclose information compiled for law enforcement purposes
(b)(8) Release would disclose information concerning the regulation of financial institutions
(b)(9) Release would disclose geological or geophysical information concerning wells

Deed of Gift Restrictions

C(1) Closed by Executive Order 13526, governing access to national security information
C(2) Closed by statute or by the agency which originated the information
C(3) Closed in accordance with restrictions contained in donor's deed of gift [formerly listed as only C]
PRM. Removed as a personal record misfile

Presidential Records Act - [44 U.S.C. 2204(a)]

P-2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]

CLARIFICATION OF FORM 4193 AND EQUIVALENT
SCI NONDISCLOSURE AGREEMENTS

Please be advised that, in conformance with the order of the United States District Court for the District of Columbia, the following is substituted for the term "classifiable" in all Sensitive Compartmented Information (SCI) nondisclosure agreements containing that term:

" . . . information that is unmarked classified information, including oral communications, and unclassified information that meets the standards for classification and is in the process of a classification determination . . . "

By making this substitution, the Director of Central Intelligence is clarifying that SCI nondisclosure agreements that contain the term "classifiable" do not cover currently unclassified information that may be subject to classification at some future date, but is not currently in the process of a classification determination. Therefore, the only circumstances under which a signatory might violate the terms of an SCI nondisclosure agreement by disclosing unclassified information are when a signatory knows, or reasonably should know, that such information is in the process of a classification determination and requires interim protection as provided in section 1.1(c) of Executive Order 12356 or any other statute or Executive order that requires interim protection for certain unclassified information while a classification determination is pending.

Thus, a signatory of an SCI nondisclosure agreement containing the word "classifiable" may be liable for disclosing information falling within the substituted phrase if:

(a) He or she knows that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, whether the unauthorized disclosure is willful or negligent; or

(b) He or she should know that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, in which case the unauthorized disclosure is negligent. In no instance could a signatory be liable for violating nondisclosure

provisions by disclosing unmarked information when, at the time of the disclosure, there was no basis to suggest, other than pure speculation, that the information was classified or in the process of a classification determination.

Through this notice, signatories to SCI nondisclosure agreements that contain the term "classifiable" are advised that their continued access to SCI will be governed by the SCI nondisclosure agreement they signed as it has been amended by this notice, without any further action.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

October 26, 1988

MEMORANDUM FOR NSC STAFF MEMBERS AND OTHER UNITED STATES
GOVERNMENT PERSONNEL

FROM: PAUL SCHOTT STEVENS *PS*
SUBJECT: Special Access Program Nondisclosure Agreements

As a condition of access to information protected by one or more Special Access Programs (SAPs), you have been asked to sign one or more SAP nondisclosure agreements.

Pursuant to a recent order of the United States District Court for the District of Columbia, the language of any such agreements containing the word "classifiable" has been clarified, as the attached notice (two copies) indicates.

To indicate that you have received the attached notice, please sign and date one copy and return it by October 31, 1988 to:

Brian Merchant
Assistant Security Officer
NSC Secretariat
Rm. 379, Old Executive Office Building
Washington, D.C. 20506

The second copy of the notice is for your records.

Attachments

NOTICE

TO NATIONAL SECURITY COUNCIL PERSONNEL AND OTHER UNITED STATES GOVERNMENT PERSONNEL WHO HAVE SIGNED SPECIAL ACCESS PROGRAM NONDISCLOSURE AGREEMENTS

Please be advised that in conformance with a recent order of the United States District Court for the District of Columbia and in order to clarify the scope of some of the language in previously executed copies of Special Access Program Nondisclosure Agreements, the following is substituted for the term "classifiable" in all nondisclosure agreements for Special Access Programs (SAP) containing that term:

" . . . information that is unmarked classified information, including oral communications, and unclassified information that meets the standards for classification and is in the process of a classification determination . . . "

Scope of classified information: This substitution clarifies that SAP nondisclosure agreements that contain the term "classifiable" do not cover currently unclassified information that may be subject to classification at some future date, but is not currently in the process of a classification determination. Therefore, the only circumstances under which a party might violate the terms of an SAP nondisclosure agreement by disclosing unclassified information are when a party knows, or reasonably should know, that such information is in the process of a classification determination and requires interim protection as provided in section 1.1(c) of Executive Order 12356 or any other statute or Executive order that requires interim protection for certain unclassified information while a classification determination is pending.

Basis for liability: A party to an SAP nondisclosure agreement containing the word "classifiable" may be liable for disclosing information falling within the substituted phrase if:

(a) He or she knows that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, whether the unauthorized disclosure is willful or negligent; or

(b) He or she should know that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, in which case the unauthorized disclosure is negligent. In no instance could a party be liable for violating

nondisclosure provisions by disclosing unmarked information when, at the time of the disclosure, there was no basis to suggest, other than pure speculation, that the information was classified or in the process of a classification determination.

Through this notice, parties to SAP nondisclosure agreements that contain the term "classifiable" are advised that their continued access to SAP information will be governed by the SAP nondisclosure agreement they signed as it has been amended by this notice, without any further action.

Signature

George VanEron

Name

George VanEron

Date

10-27-88

NOTICE

TO NATIONAL SECURITY COUNCIL PERSONNEL AND OTHER UNITED STATES GOVERNMENT PERSONNEL WHO HAVE SIGNED SPECIAL ACCESS PROGRAM NONDISCLOSURE AGREEMENTS

Please be advised that in conformance with a recent order of the United States District Court for the District of Columbia and in order to clarify the scope of some of the language in previously executed copies of Special Access Program Nondisclosure Agreements, the following is substituted for the term "classifiable" in all nondisclosure agreements for Special Access Programs (SAP) containing that term:

". . . information that is unmarked classified information, including oral communications, and unclassified information that meets the standards for classification and is in the process of a classification determination . . ."

Scope of classified information: This substitution clarifies that SAP nondisclosure agreements that contain the term "classifiable" do not cover currently unclassified information that may be subject to classification at some future date, but is not currently in the process of a classification determination. Therefore, the only circumstances under which a party might violate the terms of an SAP nondisclosure agreement by disclosing unclassified information are when a party knows, or reasonably should know, that such information is in the process of a classification determination and requires interim protection as provided in section 1.1(c) of Executive Order 12356 or any other statute or Executive order that requires interim protection for certain unclassified information while a classification determination is pending.

Basis for liability: A party to an SAP nondisclosure agreement containing the word "classifiable" may be liable for disclosing information falling within the substituted phrase if:

(a) He or she knows that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, whether the unauthorized disclosure is willful or negligent; or

(b) He or she should know that the unmarked information is classified, or meets the standards for classification and is in the process of a classification determination, in which case the unauthorized disclosure is negligent. In no instance could a party be liable for violating

nondisclosure provisions by disclosing unmarked information when, at the time of the disclosure, there was no basis to suggest, other than pure speculation, that the information was classified or in the process of a classification determination.

Through this notice, parties to SAP nondisclosure agreements that contain the term "classifiable" are advised that their continued access to SAP information will be governed by the SAP nondisclosure agreement they signed as it has been amended by this notice, without any further action.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

VAN ERON

7661

October 25, 1988

MEMORANDUM FOR NSC SENIOR DIRECTORS

FROM: PAUL SCHOTT STEVENS *PS*
SUBJECT: Security Classification Designation -
National Security Information

Executive Order No. 12356 (National Security Information) stipulates that national security information should be classified Top Secret, Secret, or Confidential. The Executive Order specifically prohibits the use of any other term to identify classified information, except as otherwise provided by statute.

The Executive Order directs the Director, Information Security Oversight Office (ISOO) to implement and monitor a uniform system for classifying, declassifying, and safeguarding national security information. In carrying out this responsibility, ISOO recently completed a survey of the NSC's implementation of the Executive Order. The ISOO representative noted that a few NSC originated classified documents, though properly bearing an authorized security classification term, also included an unauthorized added notation of "-Sensitive."

Your assistance in ensuring that only authorized security classification terms are used to identify national security information would be appreciated.

UNCLASSIFIED
NSC/S PROFILE

RECORD ID: 8807072
RECEIVED: 30 SEP 88 12

TO: STEVENS

FROM: GARFINKEL, S

DOC DATE: 29 SEP 88
SOURCE REF:

KEYWORDS: SECURITY

PERSONS:

SUBJECT: ISSUANCE BY INFORMATION SECURITY OVERSIGHT OFFICE OF NEW CLASSIFIED
INFORMATION NONDISCLOSURE AGREEMENT STANDARD FORM 312

ACTION: PREPARE MEMO FOR STEVENS DUE DATE: 04 OCT 88 STATUS: S

STAFF OFFICER: ROSTOW LOGREF:

FILES: WH NSCIF: CODES:

DOCUMENT DISTRIBUTION

FOR ACTION
ROSTOW

FOR CONCURRENCE
LEVIN
MCCUE
MENAN
MERCHANT
VAN ERON

FOR INFO
PERITO
STEVENS

COMMENTS: _____

DISPATCHED BY _____ DATE _____ BY HAND W/ATTCH

OPENED BY: NSJEC CLOSED BY: DOC 1 OF 1

UNCLASSIFIED



Information Security Oversight Office
Washington, DC 20405



7072

September 29, 1988

Dear Mr. Stevens:

The purpose of this letter is two-fold. First, it announces the issuance by the Information Security Oversight Office (ISOO) of a new "Classified Information Nondisclosure Agreement," the Standard Form 312. Second, it advises you of a clarification to previously executed copies of the Standard Form 189, also entitled "Classified Information Nondisclosure Agreement," and your requirement to communicate this clarification no later than October 27, 1988, to all employees who have previously executed the SF 189.

I. The Standard Form 312

In accordance with National Security Decision Directive 84 (NSDD 84), dated March 11, 1983, ISOO has today issued a rule that implements the Standard Form 312, "Classified Information Nondisclosure Agreement (SF 312). Effective immediately, the SF 312 shall serve as the instrument to fulfill the following requirement found in Paragraph 1(a) of NSDD 84: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access."

On December 29, 1987, ISOO imposed a moratorium on the further execution of nondisclosure agreements issued to implement NSDD 84. With respect to the SF 312, that moratorium is now lifted. Further, on August 21, 1987, ISOO imposed a moratorium on the withdrawal of access and security clearances of persons who are required to execute a nondisclosure agreement as a condition of access to classified information but who refuse to do so. With respect to the required execution of the SF 312, that moratorium also is lifted.

ISOO has issued the SF 312 to replace both the Standard Form 189, "Classified Information Nondisclosure Agreement" (SF 189), and the Standard Form 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)" (SF 189-A). However, executed copies of both the SF 189 and the SF 189-A remain valid, and fulfill that requirement of NSDD 84 quoted above. Therefore, you are required to obtain the execution of SF 312 by only those cleared Government and non-Government employees who have not previously signed either the SF 189 or SF 189-A.

Any person who has executed the SF 189 or SF 189-A may elect, however, to substitute a signed SF 312 for the previously executed agreement. You must take all reasonable steps to notify affected employees of this option, and, when an employee exercises it, to replace the previously signed nondisclosure agreement with the executed SF 312. ISOO strongly suggests the use of the enclosed "Notice to Employees," or a similar notice, for this purpose.

II. Modification of the SF 189

In accordance with a recent ruling of the United States District Court for the District of Columbia, ISOO has included in today's rule a provision that strikes the word "classifiable" from Paragraph 1 of each executed copy of the SF 189, while substituting language that clarifies the scope of "classified information," as used in the agreement. The rule also provides a definition of the scope of the term "classified information" in the SF 312, SF 189 and SF 189-A, and recites the basis for liability for violating any of these agreements. These references assure consistency in the enforcement of any of these agreements that implement NSDD 84.

On Friday, September 23, 1988, the court denied the Government's motion to substitute constructive notice through publication in the Federal Register for personal notice to every affected employee. Under the court's order, the Government must notify every employee who has executed the SF 189 of this clarification no later than October 27, 1988. When logistical circumstances do not permit compliance within that time frame for particular individuals, you should continue with efforts to notify them as quickly as possible. To assist you in meeting this notification requirement, we enclose a copy of a suggested notice, which is based upon the rule issued today. This notice, or one based upon it, may be reproduced in any format, and distributed as required. No actual physical alteration of the executed SF 189s is necessary, nor are agencies required to obtain receipts from employees that they have received notice.

The court order does not require that you notify former employees of this clarification, and, in the interest of seeking the most timely compliance, ISOO is also not imposing this requirement. Even without this notice, copies of the SF 189 executed by former employees will be enforced as the language in Paragraph 1 has been clarified.

ISOO is printing an initial stock of the SF 312 for distribution to the agencies. We will be working with your liaison to ISOO to make these arrangements. You should procure additional copies of the SF 312 through regular supply channels.

We enclose for your information and use a copy of the rule published in the Federal Register today that implements the SF 312, strikes the word "classifiable" and otherwise clarifies Paragraph 1 of the SF 189; ten sample copies of the SF 312; a copy of ISOO's suggested "Notice for Employees," taken from the published rule; and a series of questions and answers that should help answer many of your questions and the questions of employees that will arise regarding the SF 312. We are currently working on the production of a videotape and booklet that should prove to be useful briefing aids on the SF 312. We will notify you when they become available.

Please keep your ISOO liaison informed of the actions taken by your agency to implement the requirements set forth in this letter and rule. For answers to your questions, please contact ISOO at FTS 535-7251, or (202) 535-7251.

Sincerely,


Steven Garfinkel
Director

The Honorable
Paul Schott Stevens
Executive Secretary
National Security Council
The White House
Washington, DC 20500

Enclosures



Information Security Oversight Office
Washington, DC 20405



STANDARD FORM 312
CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

QUESTION	PAGE NO.
WHAT IS THE INFORMATION SECURITY OVERSIGHT OFFICE (ISOO)?.....	3
WHAT IS THE PURPOSE OF A NONDISCLOSURE AGREEMENT?.....	3
UPON WHAT LEGAL AUTHORITY IS THE SF 312 BASED?.....	4
WHO MUST SIGN THE SF 312?.....	4
ARE ALL MEMBERS OF CONGRESS, AS CONSTITUTIONALLY ELECTED OFFICE-HOLDERS, ENTITLED TO UNLIMITED ACCESS TO CLASSIFIED INFORMATION?.....	5
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?.....	5
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?.....	6
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?.....	6
HOW MUCH TIME SHOULD AN AGENCY OR CONTRACTOR PROVIDE AN EMPLOYEE TO DECIDE WHETHER TO SIGN THE SF 312?.....	7
WHAT STEPS SHOULD BE TAKEN IF A PERSON WHO HAS NOT SIGNED EITHER THE SF 189 OR SF 189-A REFUSES TO SIGN THE SF 312?.....	8
HOW DOES THE SF 312 DIFFER FROM THE SF 189 AND SF 189-A?.....	9
FOR PURPOSES OF THE SF 312, WHAT IS "CLASSIFIED INFORMATION"?.....	10
WHAT IS THE THRESHOLD FOR LIABILITY FOR VIOLATING THE NONDISCLOSURE PROVISIONS OF THE SF 312?.....	10

WHY WAS THE TERM "CLASSIFIABLE" NOT INCLUDED IN THE SF 312?.....	11
MAY THE LANGUAGE OF THE SF 312 BE ALTERED TO SUIT THE PREFERENCES OF AN INDIVIDUAL SIGNER?.....	11
DOES THE SF 312 CONFLICT WITH THE "WHISTLEBLOWER" STATUTE?.....	12
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?.....	12
HOW LONG DO AGENCIES AND CONTRACTORS HAVE TO FULFILL THE REQUIREMENT TO IMPLEMENT THE EXECUTION OF THE SF 312 BY CLEARED EMPLOYEES?.....	13
WHAT KIND OF BRIEFING OR OTHER INFORMATION SHOULD AN AGENCY OFFER AT THE TIME A PERSON IS ASKED TO SIGN THE SF 312?.....	14
IF A PERSON WHO HAS PREVIOUSLY SIGNED THE SF 189 OR SF 189-A OPTS TO SIGN AND SUBSTITUTE THE SF 312, MUST HE OR SHE ALSO RECEIVE ANOTHER BRIEFING?.....	14
WHAT STEPS MUST AN AGENCY OR CONTRACTOR TAKE TO SUBSTITUTE A SIGNED SF 312 FOR A SIGNED SF 189 OR SF 189-A? IF REQUESTED, MUST THE AGENCY OR CONTRACTOR RETURN THE PREVIOUSLY SIGNED FORM TO THE SIGNATORY?.....	15
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?.....	15
MAY THE SIGNER KEEP A COPY OF THE EXECUTED SF 312?.....	16

Q: What is the Information Security Oversight Office?

A: The Information Security Oversight Office (ISOO), established by Executive Order 12065 (December 1, 1978) and continued under Executive Order 12356 (April 6, 1982), 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.

Q: What is the purpose of a nondisclosure agreement?

A: The primary purpose of a nondisclosure agreement 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 unauthorized disclosures or to discipline employees responsible for such disclosures by initiating a civil or administrative action.

Q: Upon what legal authority is the SF 312 based?

A: 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.

Q: Who must sign the SF 312?

A: 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.

Q: Are all Members of Congress, as constitutionally elected office-holders, entitled to unlimited access to classified information?

A: No. Access to classified information is a function of three pre-conditions: 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.

Q: 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?

A: 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.

Q: 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?

A: 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.

Q: 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?

A: Since every cleared person must sign a nondisclosure agreement, the routine answer to this question is "yes." However, in implementing this program, ISOO has learned of a number of cleared employees who questioned executing a nondisclosure agreement on the basis that they had 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. In these situations, the agency or contractor must be prepared to justify the need for the clearance, since the affected employee may continue to resist executing the SF 312 on the basis that he or she has not had access to classified information.

Q: How much time should an agency or contractor provide an employee to decide whether to sign the SF 312?

A: In all situations, the answer to this question should be governed by what is reasonable under the circumstances. The following examples are illustrative. Because examples such as these and others may result in adversarial proceedings, written documentation of the transaction between the agency/contractor and the employee is critical. Also, in any situation in which there is a delay in the execution of the SF 312, the employee should be briefed on the criminal, civil or administrative consequences that may result from the unauthorized disclosure of classified information, even though the individual has not signed a nondisclosure agreement.

Example I: An employee declares explicitly that under no circumstances will he or she execute the SF 312. He or she should be advised again of the consequences of that decision. If he or she maintains the same position, the agency or contractor should take immediate steps to deny further access to classified information and to initiate the revocation of the clearance.

Example II: An employee requests additional time to consider his or her decision. He or she should be afforded a reasonable period of time to do so. If the requested additional time is 15 days or less, the agency or contractor should ordinarily grant it and make a written record of the established deadline. If the requested period of time is greater than 15 days, what that period of time will be should be discussed between the agency/contractor and employee, and a decision made, recorded, and communicated to the employee before the time begins.

Example III: An employee requests an opportunity to consult with outside counsel. He or she should be afforded a reasonable period of time in which to do so. What that period of time will be should be discussed between the agency/contractor and employee, and a decision made, recorded, and communicated to the employee before the time begins.

Example IV: An employee submits questions about the SF 312, which are reasonable both in number and in content, and requests written answers. He or she should be given a reasonable time to review those answers before any action adverse to the employee is undertaken. If the requested additional time after receipt of the answers is 15 days or less, the agency or contractor should ordinarily grant it and make a written record of the established deadline. If the requested period of time is greater than 15 days, what that period of time will be should be discussed between the agency/contractor and employee, and a decision made, recorded, and communicated to the employee before the time begins.

Q: What steps should be taken if a person who has not signed either the SF 189 or SF 189-A refuses to sign the SF 312?

A: 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.

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

A: 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.

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

A: 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.

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

A: 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.

Q: Why was the term "classifiable" not included in the SF 312?

A: The term "classifiable," as originally used in Paragraph 1 of the SF 189, was not included in the SF 312 to avoid the confusion that arose over the intended scope of that word. The "able" suffix in the word "classifiable" promoted the incorrect interpretation that the word referred to unclassified information that might be classified in the future. Rather, the term "classifiable information" was intended and defined to encompass two narrow classes of information that must be protected under Executive Order 12356, "National Security Information." These are (a) unmarked classified information, including oral communications; and (b) unclassified information that meets the standards for classification and is in the process of a classification determination. In response to a recent order of the United States District Court for the District of Columbia, the word "classifiable" has now been struck from the SF 189 and replaced with language consistent with its previously published definition. The same language is included in the SF 312. Further, in accordance with a rule issued by the Information Security Oversight Office, the SF 189 and the SF 189-A shall be interpreted and enforced in a manner that is fully consistent with the interpretation and enforcement of the SF 312.

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

A: 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.

Q: Does the SF-312 conflict with the "whistleblower" statute?

A: The SF 312 does not conflict with the "whistleblower" statute (5 U.S.C. § 2302). The statute does not extend its protection to 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 employees 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.

Q: 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?

A: 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.

Q: How long do agencies and contractors have to fulfill the requirement to implement the execution of the SF 312 by cleared employees?

A: In issuing the SF 312, ISOO is not establishing at this time a firm deadline for full agency and contractor compliance. However, ISOO encourages agencies that are responsible for Government and non-Government compliance to impose deadlines consistent with logistical realities. ISOO will continue to monitor agency compliance to help ensure that full implementation is achieved in a timely manner.

Further, it should be noted that the effort to achieve full compliance within Government agencies should not be particularly burdensome. At the time ISOO imposed a moratorium on the execution of further copies of the SF 189 at the end of 1987, agencies had reported compliance that approximated 98-99% of the persons required to execute the nondisclosure agreement. To achieve full compliance within Government agencies will require the execution of the SF 312 by the remaining one or two percent of employees; by those employees who have been cleared for access to classified information since the imposition of the moratorium; and by newly cleared employees.

ISOO does not have comparable data for the degree of compliance within industry at the time of the imposition of the moratorium. The Defense Investigative Service and other agencies that are responsible for the security administration of classified contracts, licenses and grants should establish deadlines for full compliance.

Q: What kind of briefing or other information should an agency offer at the time a person is asked to sign the SF 312?

A: At the time an employee is asked to sign the SF 312, the agency or contractor should provide a briefing that, at a minimum, provides information about: (a) the purposes of the nondisclosure agreement; (b) the intent and scope of its provisions; (c) the consequences that will result from the employee's failure to sign the agreement; and (d) the consequences that may result from the unauthorized disclosure of classified information, including possible administrative, civil, or criminal sanctions. In this context, the briefing should explain clearly the procedures to be followed in ascertaining whether a prospective recipient may have access to classified information.

The briefing may be limited to the subject of the SF 312, or it may be in the context of an initial or refresher briefing about the information security system, generally. While the heart of the briefing may be based upon a prepared text or audiovisual, the agency or contractor representative should answer any reasonable questions or concerns raised by the individual regarding the SF 312, or be prepared to obtain answers to those questions. The representative must also have available copies of every statute, executive order or regulation that is referenced in Paragraph 10 of the SF 312.

Q: If a person who has previously signed the SF 189 or SF 189-A opts to sign and substitute the SF 312, must he or she also receive another briefing?

A: The agency or contractor is not required to provide an additional briefing upon execution of the SF 312 in these circumstances. However, the agency or contractor representative should answer any reasonable questions or concerns raised by the individual regarding the SF 312, or be prepared to obtain answers to those questions. The representative should also have available copies of every statute, executive order or regulation that is referenced in Paragraph 10 of the SF 312.

Q: What steps must an agency or contractor take to substitute a signed SF 312 for a signed SF 189 or SF 189-A? If requested, must the agency or contractor return the previously signed form to the signatory?

A: In the event that a signatory opts to substitute a signed SF 312 for a previously signed SF 189 or SF 189-A, the agency or contractor shall dispose of the SF 189 or SF 189-A, either through its physical destruction or, if requested, through its return to the signatory, if these means of disposal can be accomplished with a reasonable amount of effort or expenditure of resources. In situations in which physical disposal is not a reasonable alternative, the agency or contractor shall take all reasonable steps to annotate the retained version of the SF 189 or SF 189-A with markings that make clear that it has been voided; and provide the signatory with an official written statement to that effect. In extraordinary circumstances in which none of the alternatives above is reasonable, the agency or contractor shall provide the signatory with an official written statement that the retained SF 189 or SF 189-A is void. In any circumstances, the SF 189 or SF 189-A should not be destroyed or voided until after the employee has executed the SF 312.

Q: 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?

A: The originals or legally enforceable facsimiles of 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.

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

A: 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.

NOTICE

**TO ALL PERSONS WHO HAVE SIGNED THE STANDARD FORM 189
"CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT"
OR THE STANDARD FORM 189-A
"CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT
(INDUSTRIAL/COMMERCIAL/NON-GOVERNMENT)"**

1. By a rule issued by the Information Security Oversight Office, published in the Federal Register on September 29, 1988, implementing an order of the United States District Court for the District of Columbia, the second sentence of Paragraph 1 of every executed copy of the Standard Form 189, "Classified Information Nondisclosure Agreement," 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. The Information Security Oversight Office has issued a new "Classified Information Nondisclosure Agreement," Standard Form 312, to be executed by all cleared Government and non-Government employees as a condition of access to classified information. The SF 312 will be used in lieu of the Standard Form 189, "Classified Information Nondisclosure Agreement," and the Standard Form 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 employee who has previously signed the SF 189 or the SF 189-A does not need to execute the SF 312. However, at that employee's discretion, he or she may elect to substitute a signed SF 312 for a previously signed SF 189 or SF 189-A.

3. Scope of "classified information": As used in the SF 312, the SF 189, and the SF 189-A, "classified information" includes 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.

4. 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: (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.

5. For further information, please contact:

Final Rule

**Thursday
September 29, 1988**

Part VI

**Information Security
Oversight Office**

32 CFR Part 2003

**National Security Information; Standard
Forms; Final Rule**

INFORMATION SECURITY OVERSIGHT OFFICE**32 CFR Part 2003****National Security Information; Standard Forms**

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Final rule.

SUMMARY: This amendment to 32 CFR 2003.20 provides for: (1) the issuance and use of Standard Form 312, "Classified Information Nondisclosure Agreement" (SF 312); and (2) the modification of Paragraph 1 of all previously executed copies of Standard Form 189, "Classified Information Nondisclosure Agreement" (SF 189), to strike the word "classifiable" and to substitute in its place language that clarifies the scope of "classified information" as used in those agreements. From the effective date of this rule, the SF 312 shall be used in lieu of its predecessor nondisclosure agreements, SF 189 and Standard Form 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)" (SF 189-A). ISOO is issuing the SF 312 as a preferred means of clarifying the scope of some language in the SF 189 and the SF 189-A that has been at issue in litigation concerning the constitutionality and legality of certain nondisclosure agreements, including the SF 189. Notwithstanding the changes in some of its language, the SF 312 does not in any way differ from its predecessor nondisclosure agreements with respect to the substance of the information that each is intended to protect. ISOO is clarifying executed copies of the SF 189 to comply with a recent order of the United States District Court for the District of Columbia, to take account of statutory provisions that reflect congressional concern regarding possible ambiguity of the word "classifiable," and to make the language of the SF 189 more consistent with the language of the SF 312 and the SF 189-A.

EFFECTIVE DATE: September 29, 1988.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO, 202-535-7251.

SUPPLEMENTARY INFORMATION: This amendment to 32 CFR Part 2003 is issued pursuant to section 5.2(b)(7) of Executive Order 12356, "National Security Information," which grants the Director of ISOO the authority to issue standardized security forms, and Paragraph 1 of National Security Decision Directive 84, March 11, 1983,

which directs ISOO to issue a standardized nondisclosure agreement to be signed as a condition of access by all persons cleared for access to classified information. In fulfilling this requirement, ISOO has previously issued two nondisclosure agreements: SF 189, "Classified Information Nondisclosure Agreement," in September 1983; and SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)," in November 1986.

On December 29, 1987, ISOO directed agencies to halt further implementation of the SF 189 and SF 189-A as a result of the enactment of section 630 of the Treasury, Postal Service, and General Appropriations Act, 1988, which was part of the Omnibus Continuing Resolution for Fiscal Year 1988 (Pub. L. 100-202). On May 27, 1988, in litigation primarily involving the constitutionality and legality of the SF 189, the United States District Court for the District of Columbia ruled that Section 630 of Public Law 100-202 is unconstitutional (*National Federation of Federal Employees v. United States, et al.*, Civil Action No. 87-2284-OG; *American Federation of Government Employees, et al. v. Garfinkel, et al.*, Civil Action No. 87-2412-OG; *American Foreign Service Association, et al. v. Garfinkel, et al.*, Civil Action No. 88-0440-OG). In a subsequent ruling of July 28, 1988, in the first two of the above-captioned cases, the same court upheld the constitutionality and legality of the SF 189. However, the court also ruled that in order to bring the scope of the word "classifiable" within constitutional limits, the SF 189 must be modified, either (a) by providing each signatory a copy of ISOO's definition of "classifiable information," as published in 52 FR 48367 on December 21, 1987; or (b) by striking the word from executed copies of the agreement. Notwithstanding these rulings upholding the validity of the predecessor nondisclosure agreements, ISOO has concluded that, in lifting the moratorium on the execution of required nondisclosure agreements, a preferred means to deal with the perceived ambiguities in their language is the issuance of a new nondisclosure agreement, the SF 312. The SF 312 avoids as many of these perceived problem areas as possible without changing the substance of the classified information that the nondisclosure agreement is intended to protect. In issuing the SF 312, ISOO does not seek its execution by every cleared Government or industry employee who has already executed an SF 189 or an SF 189-A, since these total over two million

individuals. However, the rule provides that every individual who previously signed an SF 189 or SF 189-A may substitute a signed copy of the SF 312 at his or her own choosing. Also, through this rule ISOO is instructing agencies to enforce the predecessor agreements in a manner that is fully consistent with the enforcement of the SF 312. To help achieve greater consistency, ISOO is complying with the court order by opting to strike the word "classifiable" from the SF 189, while substituting language that clarifies the scope of "classified information," as used in the agreement. This language is taken from the definition of "classifiable" previously published in the Code of Federal Regulations, and adjudged by the District Court to bring the definition within constitutional and legal standards. ISOO has not included the word "classifiable" in the SF 312, and did not previously include it in the SF 189-A, although these agreements are both intended to protect the same information protected by the SF 189. The word "classifiable" had been included in the SF 189 not to introduce concepts separate and distinct from classified information, but to emphasize the need to protect unmarked classified information and information in the process of a classification determination. Therefore, striking the word from the SF 189 is the more consistent of the two options presented by the court, while its concepts remain protected within the scope of classified information.

Concurrent with the issuance of the SF 312, by a letter of this date the ISOO Director is instructing the senior official for information security oversight in each agency that creates or handles classified information to lift the current moratorium on the execution of the "Classified Information Nondisclosure Agreement," imposed by letter of December 29, 1987; and to lift the moratorium on the withdrawal of access to classified information and security clearances, imposed by letter of August 21, 1987, for those cleared persons who refuse to sign the SF 312.

Before issuing the SF 312, ISOO submitted drafts for review and comment to the executive branch agencies most affected by it; to seven Committees or Subcommittees of the Congress most involved with the subject of classified information; and to selected interest groups actively concerned with this subject. ISOO has considered those comments that it has received in response to its solicitations, and, when ISOO concluded that suggested changes were warranted, it has incorporated

these into the SF 312 or this implementing rule. As required by National Security Decision Directive 84, the Department of Justice has concluded that the SF 312 is enforceable in a civil action brought by the United States.

This is not a major rule for purposes of Executive Order 12291.

List of Subjects in 32 CFR Part 2003

Classified information, Executive orders, Information, National security information, Security information.

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, September 29, 1988, 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.

Dated: September 23, 1988.
Steven Garfinkel,
Director, Information Security Oversight
Office.

[FR Doc. 88-22232 Filed 9-26-88; 8:45 am]
BILLING CODE 6820-KC-M

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Printed or typed)

_____, 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.

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)

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 I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
-----------	------	---

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)
(Type or print)

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 where 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.

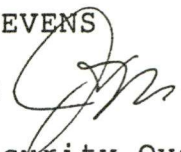
NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

4437

August 23, 1988

INFORMATION

MEMORANDUM FOR PAUL SCHOTT STEVENS

FROM: JAMES T. McCUE 
SUBJECT: Information Security Oversight Office
(ISSO) Review of the NSC Information
Security Program

At Tab 1 is the Director, ISSO's June 13, 1988 letter advising you of their scheduled review of subject program on September 14, 15, and 16, 1988. At ISSO's request the review is now set for October 12, 13, and 14, 1988.

ISSO does not expect a formal response to their letter.

Please note that ISSO's review will focus primarily on (1) safeguarding and accountability practices; (2) security education; and (3) classification management. A reading of ISSO's 1987 review of the NSC indicates they examined only the classification management program.

The draft NSC Security Manual I submitted to you on August 19, 1988 for pre-coordination approval will, if finalized, establish requirements for accountability of Top Secret and codeword documents, as well as a security education program. The latter includes an initial briefing and an annual refresher briefing. Presently, such briefings are virtually nonexistent. For the past couple of months the USSS gave new passholders an initial security briefing; however, I believe that program is on hold for awhile.

cc: George Van Eron
Nancy Menan



Information Security Oversight Office
Washington, DC 20405



4437

June 13, 1988

Dear Mr. Stevens:

Under Executive Order 12356, "National Security Information," the Information Security Oversight Office (ISOO) oversees the executive branch information security system. Section 5.2(b)(4) of the Order grants the Director of ISOO authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information. This section also authorizes the Director to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities.

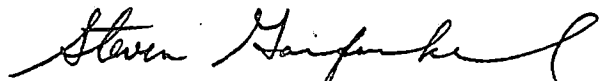
In accordance with this authority, Thomas R. Martin, ISOO Program Analyst, will review the information security program in the National Security Council (NSC) on September 14, 1988. This date has been coordinated with James T. McCue, Director of Security Programs. The review will focus primarily on (1) safeguarding and accountability practices; (2) security education; and (3) classification management.

In continuance of its detailed reviews of the classified product being generated by executive branch agencies, on September 15 and 16, 1988, ISOO will conduct a special document review of the NSC's classified product. Specifically, the review will focus on classification, declassification, marking and dissemination as prescribed by the Order. The document review team, consisting of Mr. Martin and Rudolph Waddy, would like to review a minimum of 300 documents with a desired goal of 500 documents. These documents should consist of letters, memoranda, studies, working papers, etc. An outbriefing by the ISOO analysts is encouraged and can be conducted upon completion of the review if desired.

TAB I

Information concerning Messrs. Martin and Waddy's security clearances are enclosed and can be verified by contacting June Brown, ISOO Security Manager, on 535-7255. If you have any questions about the scope of the compliance or document reviews, please contact Mr. Martin on 535-7256. Thank you for your cooperation in this matter.

Sincerely,


Steven Garfinkel
Director

The Honorable
Paul Schott Stevens
Executive Secretary
National Security Council
The White House
Washington, DC 20500

Enclosures

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
02. Memorandum	For Paul Schott Stevens From: ISOO Re: Request for visit approval (1 pp.)	6/13/88	(b)(6)	

Collection:

Record Group: Bush Presidential Records
Office: National Security Council
Series: H-Files
Subseries: Transition Files
WHORM Cat.:
File Location: NSC Procedural Manual - Binder 1 [2]

Date Closed: 9/4/2019	OA/ID Number: 99017-002
FOIA/SYS Case #: 2019-1493-S	Appeal Case #:
Re-review Case #:	Appeal Disposition:
P-2/P-5 Review Case #:	Disposition Date:
AR Case #:	MR Case #:
AR Disposition:	MR Disposition:
AR Disposition Date:	MR Disposition Date:

RESTRICTION CODES

Freedom of Information Act (FOIA) - [5 U.S.C. 552(b)]

- (b)(1) National security classified information
- (b)(2) Release would disclose internal personnel rules and practices of an agency
- (b)(3) Release would violate a Federal statute
- (b)(4) Release would disclose trade secrets or confidential or financial information
- (b)(6) Release would constitute a clearly unwarranted invasion of personal privacy
- (b)(7) Release would disclose information compiled for law enforcement purposes
- (b)(8) Release would disclose information concerning the regulation of financial institutions
- (b)(9) Release would disclose geological or geophysical information concerning wells

Deed of Gift Restrictions

- C(1) Closed by Executive Order 13526, governing access to national security information
- C(2) Closed by statute or by the agency which originated the information
- C(3) Closed in accordance with restrictions contained in donor's deed of gift [formerly listed as only C]
- PRM. Removed as a personal record misfile

Presidential Records Act - [44 U.S.C. 2204(a)]

- P-2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]

Facility to be visitedVarious NSC information security programs**Duration of visit**Fiscal Year 88**Purpose of Visit**ISOO Document Review and Program Inspection**Person to be contacted**Mr. James T. McCue

2. Approval is assumed in the absence of contrary advice.



June T. Brown
Security Manager
535-7255

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

August 8, 1988

ACTION

MEMORANDUM FOR PAUL SCHOTT STEVENS

FROM: JAMES T. MCCUE *JT*
SUBJECT: Personnel Security Procedures

At Tab 2 is a copy of your April 7, 1988 memorandum establishing the security policy to be followed with respect to the Entry on Duty (EoD) of military and civilian candidates selected for positions with the NSC.

You asked me, in cooperation with George Van Eron, Mary Dix and Carol Paquette, to draw up for your review a minimum set of procedures that can be provided to Senior Directors for use in handling new hires within their directorates.

At Tab 1 is the result of our effort. The procedures are designed to create a reasonable personnel security program without imposing an unbearable administrative burden on Senior Directors. Please note that the procedures address candidates, including consultants, with and without the requisite clearances. This is because you require all candidates to receive a security interview prior to their interview with you.

CP
Carol Paquette, *JT* George Van Eron and *MD* Mary Dix concur.

RECOMMENDATION

That you approve/sign the memorandum at Tab 1 forwarding procedures which implement your memorandum at Tab 2 establishing the policy on personnel security requirements for entry-on-duty with the NSC.

Approve _____

Disapprove _____

Attachments

- Tab 1 - Your Memorandum for NSC Senior Directors
- Tab 2 - Your April 7, 1988 Memorandum

NATIONAL SECURITY COUNCIL

WASHINGTON, D.C. 20506

MEMORANDUM FOR NSC SENIOR DIRECTORS

FROM: PAUL SCHOTT STEVENS

SUBJECT: Personnel Security Procedures

The memorandum at attachment 2 directed that procedures be provided to all NSC Senior Directors which will be used for determining the Entry-on-Duty (EoD) eligibility of selectees, civilian and military, who do not have the requisite Top Secret (TS) security clearance and Sensitive Compartmented Information (SCI) access authorization. These procedures are described at attachment 1. The latter also describes security procedures to be followed for the EoD of those selectees who have the requisite clearance and access authorization. The procedures apply to "candidates", "selectees", and "passholders". Selectees will not be eligible to commence employment with the NSC until they have a TS clearance and are eligible for SCI indoctrination. Exceptions to this requirement are described below.

For purpose of clarification, a "candidate" is an applicant whose qualifications make them tentatively qualified for detail, assignment, or employment at the NSC. Once the candidate has been approved for such detail, assignment, or employment, they become a "selectee" until such time as they EoD with the NSC, at which time they become a "passholder".

Consultants whose services are acquired in the same manner as civilian direct hire employees of the NSC must meet the same personnel security requirements as selectees.

Because of the nature of the work carried out by the NSC, it is necessary that all selectees either have the required clearances and accesses, or can be granted these clearances and accesses upon their EoD. In the few instances where there is a defined requirement for an exception to this policy, as elaborated on in attachment 1, the following procedures are to be followed:

- The Director, NSC Security Programs (D/NSCSP) shall identify to the Director of Administration, NSC or to the Director of Resources, White House Situation Support Staff (WHSSS), hereafter referred to interchangeably as the "Administrator", depending on whether the detail, assignment, or employment is WHSSS or other NSC Directorates, those candidates who do not have or are not immediately eligible for a TS clearance and/or SCI access.

- If the candidate cannot immediately be granted a TS clearance, the Administrator, in concurrence with the appropriate Senior Director, will request the Executive Secretary to authorize the Director, NSC Security Programs to grant an Interim Top Secret (ITS) clearance, provided the required investigation has been initiated and there is no security justification precluding granting such clearance. This request will be incorporated in the Administrator's memorandum to the Executive Secretary recommending selection of the candidate.

- In exceptional cases, where the passholder has a TS clearance but requires a current Full Field Investigation (FFI) to qualify for SCI indoctrination, a "Compelling Need" request shall be submitted to the D/NSCSP by the Administrator. Under this authority, passholders who have a final TS certified to by the D/NSCSP but require an updated FFI for SCI indoctrination eligibility, may be eligible for early SCI indoctrination based on a justified "compelling need" established by the Administrator. Under this option, once a determination of the necessity for early access to SCI has been made, the Administrator may, with the concurrence of the Executive Secretary, submit a memorandum to the D/NSCSP, subject: "Compelling Need Request for Access to SCI by (name of employee)." A passholder entering-on-duty without an SCI access authorization shall be denied access to:

- Secure voice communications.
- Security cabinets containing SCI.
- Lock combinations to security cabinets containing SCI.
- Computers containing SCI material.
- Passwords to computers which contain SCI material.
- SCI material via the mail distribution system or messenger system.
- The cipher system code for controlling entry to the SCIF.
- Controlling ingress to the SCIF.
- The new staff member must be under continuous escort by an SCI indoctrinated coworker.

Attachments

1. Personnel Security Procedures
2. Executive Secretary Memorandum of April 7, 1988

Personnel Security Procedures

1. General

a. Unless a Full Field Investigation (FFI) has been accomplished within the past twelve months by an accredited investigative agency, all personnel assigned to the White House Complex are required, for suitability purposes, to undergo an FFI by the Federal Bureau of Investigation (FBI). The resulting report is used in determining a candidate's eligibility for a security clearance and access to Sensitive Compartmented Information (SCI).

b. The following procedures apply to all military and civilian selectees for positions with the National Security Council (NSC), including consultants employed in the same manner as civilian direct hire employees of the NSC, detailees from departments and agencies of the Executive Branch, management interns, and seasonal employees:

(1) Only United States citizens shall be granted a personnel security clearance and indoctrinated for access to Sensitive Compartmented Information (SCI). All permanent passholders require a TOP SECRET (TS) security clearance and must be eligible for indoctrination to SCI. Temporary passholders with a favorable National Agency Check and a pending FBI FFI may, if otherwise eligible, be granted an INTERIM TS (ITS) security clearance in accordance with the procedures in paragraph 2. b., below. Passholders with an ITS will not be eligible for SCI indoctrination until the FFI is completed and they have been granted a final TS clearance.

(2) A selectee for a position with the NSC, who does not have an existing TS security clearance or recent FFI, will be subject to an FBI FFI. The length of time it takes to complete any required investigation cannot be predetermined. Although existing collateral security clearances are generally transferable between agencies of the Executive Branch; SCI authorizations are not. However, selectees holding SCI access eligibility at the time of their transfer to the NSC may continue to have access to the same categories of SCI at the NSC pending indoctrination by the Central Intelligence Agency (CIA).

(3) Passholders shall not be employed in a Sensitive Compartmented Information Facility (SCIF) until they have been indoctrinated for SCI. The reason for this prohibition is that SCIFs in the NSC contain secure voice communication systems in addition to SCI material in their ADP systems, in security cabinets and, in most cases, in daily use within the work areas. Due to the complexity of security measures to preclude unauthorized access, only SCI indoctrinated personnel shall be assigned to work in a SCIF. However, should the Director of Administration, NSC or the Director of Resources, White House Situation Support Staff, herein after referred to interchangeably as the "Administrator", depending on whether the selectee will be assigned to an NSC Directorate or White House Support Staff, determine that the procedures outlined in paragraph 2., below,

will cause an undue delay in EoD, and that it is in the national interest to permit the selectee to EoD pending completion of the requisite FFI or SCI eligibility determination, the appropriate Administrator may take the action required in paragraph 2. b. or 3. c., below.

c. The Director, NSC Security Programs (D/NSCSP) shall provide the Administrator with a written notification of the security clearance and SCI access authorization status of the selectee. The notification shall stipulate any prohibition against EoD pending completion of security clearance determinations and SCI access authorizations required for job performance in the NSC.

2. Application for a TOP SECRET Security Clearance

a. A promising candidate for a position in the NSC must complete a Standard Form 86 (Security Investigation Data for Sensitive Position) (SF 86) before receiving a security interview by the D/NSCSP. The interview addresses questions asked on the SF 86 and is designed to elicit information which will assist management in the selection process. The Executive Secretary, NSC will be advised by the D/NSCSP of any issues arising from the interview which could possibly result in denial of a TS clearance or eligibility for access to SCI. If required, additional security forms will be furnished to the selectee by the D/NSCSP.

b. The Administrator, with the concurrence of the Executive Secretary, may opt to request the selectee be granted an INTERIM TOP SECRET (ITS) clearance. The granting of an ITS is dependent upon the completion of a favorable FBI namecheck of the selectee and the initiation of the required Full Field Investigation (FFI) by the Federal Bureau of Investigation or other designated agency. Under such an option, the Administrator shall submit a written request to the D/NSCSP justifying the need for the ITS. Because the granting of an ITS clearance does not qualify a selectee for eligibility for access to SCI, this option does not apply to a selectee who is to be assigned to an area accredited by the United States Secret Service as a Sensitive Compartmented Information Facility (SCIF) in which SCI material is maintained in any configuration. After entering-on-duty with an ITS or without eligibility for indoctrination to SCI, the passholder shall be denied access to:

- (1) secure voice communications;
- (2) security cabinets containing SCI;
- (3) lock combinations to security cabinets containing SCI;
- (4) computers containing SCI material;
- (5) passwords to computers which contain SCI material;
- (6) SCI material via the mail distribution system or

messenger system and,

(7) the cipher system code for controlling entry to the SCIF. While in the SCIF, the selectee shall not control ingress to the SCIF and must be under continuous escort by an SCI indoctrinated coworker.

3. Access to Sensitive Compartmented Information (SCI)

a. Selectees detailed to the NSC from Executive Departments and Agencies where they hold the requisite SCI accesses should request their Special Security Office (SSO) to certify the accesses to the NSC through the CIA which serves as the NSC's SSO. If the selectee does hold such accesses, and will occupy an NSC position requiring certification of these accesses outside the NSC, it will be necessary for the CIA to indoctrinate/reindoctrinate the selectee after he or she has entered on duty with the NSC (CIA will not transfer SCI accesses "in status" to the NSC). Once on the CIA roster of SCI indoctrinated passholders, the CIA, as the NSC SSO, will "pass" SCI accesses to activities outside the NSC.

b. Selectees without SCI access may obtain access through the following consecutive steps:

(1) the selectee must have been the subject of a completed FFI covering the most recent fifteen years of his or her life. A FFI which meets these requirements, and is not more than five years old, will generally satisfy requirements for SCI indoctrination;

(2) a TS security clearance must have been issued, or certified to, by the D/NSCSP;

(3) approval must be received from the CIA for SCI indoctrination; and

(4) indoctrination must be completed before access to SCI is authorized.

c. On receipt of notification from the CIA that the selectee has been indoctrinated for SCI, the D/NSCSP will send a written notification to the NSC Senior Director, with an information copy to the Directorate's Security Manager, in whose office the passholder is assigned.

d. In exceptional cases, where the passholder has a TS clearance but requires a current FFI to qualify for SCI indoctrination, a "Compelling Need" request shall be submitted to the D/NSCSP by the Administrator. Under this authority, passholders who have a final TS certified to by the D/NSCSP but require an updated FFI for SCI indoctrination eligibility, may be eligible for early SCI indoctrination based on a justified "compelling need" established by the Administrator. Under this option, once a determination of the necessity for early access to SCI has been made, the Administrator may, with the concurrence of the Executive Secretary, submit a memorandum to

The D/NSCSP, subject: "Compelling Need Request for Access to SCI by (name of employee)." The request shall include:

- (1) the passholder's full name;
- (2) the passholder's date and place of birth;
- (3) the passholder's Social Security Account Number, rank/grade, and, if active duty military, branch of service;
- (4) the passholder's duty title and SCI accesses required, and
- (5) justification establishing the immediate need for access to SCI and an explanation as to why another indoctrinated passholder cannot perform the SCI related task until the passholder is granted SCI access through the normal process.

e. On receipt of the information required in d. (5)., above, the D/NSCSP will enclose the request with the submission of Form 2018a (Special Access Approval) to the CIA. A copy of the passholder's most recent SF 86 will also be included.

f. Passholder's with SCI are subject to a periodic reinvestigation every five years.

4. Consultants

Consultants are subject to the same investigative requirements as passholders if they require access to TS or SCI information. Once a prospective consultant has been tentatively approved for appointment, the D/NSCSP should be notified in order that expeditious action may be taken to identify and confirm existing clearances or to initiate any investigations considered appropriate for the level of access required.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

MEMORANDUM FOR JAMES T. MCCUE
MARY A. DIX
GEORGE VAN ERON
CAROL PAQUETTE

7 April, 1988

FROM: PAUL SCHOTT STEVENS 
SUBJECT: Security Approval Required for
Entry-on Duty

As you know, the process followed in the selection of new staff for the NSC is designed to obtain the best qualified candidates for the job. Not the least important consideration is the question of security. The NSC is, if not the primary, certainly a major target of hostile intelligence services. As a result, the NSC must take all reasonable precautions to ensure that classified information, including codeword, can be accessed only by those persons with a proper level of security clearance and an established "need-to-know." In the NSC a Top Secret clearance with codeword authorization is mandatory. Unfortunately, from a security viewpoint, it is not unusual to have several individuals on duty in the NSC who are still in the clearance process for access to Top Secret and codeword information. This situation exists because of the shortage of candidates with the required clearances. Therefore, certain security measures must be taken to prevent unauthorized access to classified and codeword information by personnel who are in the clearance process.

Effective this date, candidates for NSC positions, be they military or civilian permanent staff, detailees or consultants, who do not have current SCI clearances, will not be authorized by me to enter-on-duty with the NSC absent concurrence by the Director, NSC Security Programs provided in writing to the Director of Administration. In most instances such concurrence will require the employing directorate to adopt appropriate procedures designed to preclude access to computer terminals, secure voice communications systems, and security cabinets containing classified and codeword information to which the new employee is not yet cleared for access. Such procedures should also address handling of classified mail, document and office access controls, and other security measures applicable to the particular office involved. I ask that Jim McCue, in cooperation with George Van Eron, Mary Dix and Carol Paquette, draw up for my review a minimum set of such procedures that can be provided to Senior Directors in case of such new hires within their directorates. Implementation of such procedures will be the responsibility of the respective Senior Director and his or her designated Security Manager. Upon my approval of such procedures, Mr. McCue is requested to forward this memorandum together with such procedures to NSC Senior Directors for their information.

cc: Donley

Attachment 2

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

MEMORANDUM FOR JAMES T. MCCUE
MARY A. DIX
GEORGE VAN ERON
CAROL PAQUETTE

7 April, 1988

FROM: PAUL SCHOTT STEVENS 
SUBJECT: Security Approval Required for
Entry-on Duty

As you know, the process followed in the selection of new staff for the NSC is designed to obtain the best qualified candidates for the job. Not the least important consideration is the question of security. The NSC is, if not the primary, certainly a major target of hostile intelligence services. As a result, the NSC must take all reasonable precautions to ensure that classified information, including codeword, can be accessed only by those persons with a proper level of security clearance and an established "need-to-know." In the NSC a Top Secret clearance with codeword authorization is mandatory. Unfortunately, from a security viewpoint, it is not unusual to have several individuals on duty in the NSC who are still in the clearance process for access to Top Secret and codeword information. This situation exists because of the shortage of candidates with the required clearances. Therefore, certain security measures must be taken to prevent unauthorized access to classified and codeword information by personnel who are in the clearance process.

Effective this date, candidates for NSC positions, be they military or civilian permanent staff, detailees or consultants, who do not have current SCI clearances, will not be authorized by me to enter-on-duty with the NSC absent concurrence by the Director, NSC Security Programs provided in writing to the Director of Administration. In most instances such concurrence will require the employing directorate to adopt appropriate procedures designed to preclude access to computer terminals, secure voice communications systems, and security cabinets containing classified and codeword information to which the new employee is not yet cleared for access. Such procedures should also address handling of classified mail, document and office access controls, and other security measures applicable to the particular office involved. I ask that Jim McCue, in cooperation with George Van Eron, Mary Dix and Carol Paquette, draw up for my review a minimum set of such procedures that can be provided to Senior Directors in case of such new hires within their directorates. Implementation of such procedures will be the responsibility of the respective Senior Director and his or her designated Security Manager. Upon my approval of such procedures, Mr. McCue is requested to forward this memorandum together with such procedures to NSC Senior Directors for their information.

cc: Donley

~~CONFIDENTIAL~~

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

Blume

July 22, 1988

MEMORANDUM FOR PAUL SCHOTT STEVENS
ROBERT PERITO
✓MICHAEL DONLEY
NANCY MENAN

FROM: JAMES T. MCCUE *Jm*
SUBJECT: Classified Document Control Data Base

At Tab 1 is a copy of an ACTION memorandum which has necessitated the meeting in the Executive Secretary's office at 2:00 PM, Monday, July 25, 1988.

At Tab 2 is a copy of a March 18, 1988 memorandum to George Van Eron which resulted in the ACTION memorandum at Tab 1.

The establishment of the subject data base will not apply to the message traffic processed by the White House Situation Room.

Tab 1- Copy of ACTION Memorandum dtd July 18, 1988
Tab 2- Copy of Memorandum for George Van Eron dtd
March 18, 1988

Unclassified when Tab 1 is withdrawn

~~CONFIDENTIAL~~

DECLASSIFIED
PER NSC WAIVER, #2017-03
By *MB* NARA, Date *9/4/98*

CONFIDENTIAL

5270

July 18, 1988

ACTION

MEMORANDUM FOR PAUL SCHOTT STEVENS

FROM: JAMES T. MCCUE *JTM*

SUBJECT: Classified Document Control Data Base

ISSUE

Definition of and requirements needed to establish a computer accountability system for Top Secret and SCI documents.

The purpose of this accountability system is to establish a computer registry within each NSC directorate for use by the office security manager (or alternate) and the NSC security office. Brian Merchant is responsible for the computer design.

OBJECTIVE

The Secretariat handles an estimated 80% of the Top Secret and codeword material received by NSC or sent by NSC. This material is already handled by an accountability system. The other 20% is not necessarily entered into a manual or automated accountability system. File copies of documents generated by the NSC may or may not be incorporated into our existing system. Working papers are generally not in any accountability system even though they may be kept in storage independently. Adoption of the proposed automated accountability system would enhance the total security environment of the NSC.

DISCUSSION

The possible options available to implement this requirement are:

- develop a mainframe computer application,
- develop a VAX computer application,
- develop a stand-alone application.

Each of these options have been examined and are discussed below. Unfortunately, there is no quick solution.

CONFIDENTIAL

Declassify on: OADR

DECLASSIFIED

PER NSC WAIVER, 152017-03

By MB NARA, Date 9/4/19

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

-2-

MAIN FRAME COMPUTER APPLICATION

This option would develop a computer accountability system on the WHCA/IBM main frame computer. Requirements would have to be developed for the design of software applications and the availability of modern technology.

Therefore, NSC should task White House Communications Agency (WHCA) to examine application requirements. Once approved by WHCA, the contractor would design a DOCLOG type file which would allow for document accountability tracking.

A parallel access file controlled by a FAAAS application would be designed at the same time.

VAX COMPUTER APPLICATION

Discussions were held with WHSSS. ^{SLOW} ~~PAPER~~ They do not have the resources available to develop this application. In addition, the hardware support requires a LAN configuration across the entire staff to implement.

STAND-ALONE APPLICATION

dBase III was a possible stand-alone application. However, after discussions with IBM, dBase III does not look feasible because:

- it has very limited capability and is designed for use by one or two users,
- while it allows software design by the user, the resultant software package is not as versatile as that of a main frame application.

Concurrence: George Van Eron

RECOMMENDATION

That you sign the memorandum to Pat McGovern at Tab I.

_____ Approve

_____ Disapprove

Attachment

Tab I - Memorandum to Pat McGovern

Prepared by:
Brian T. Merchant

~~CONFIDENTIAL~~~~CONFIDENTIAL~~

5270

MEMORANDUM FOR COLONEL PATRICK MCGOVERN
WHITE HOUSE COMMUNICATIONS AGENCY

FROM: PAUL SCHOTT STEVENS

SUBJECT: Document Accountability System

It is requested that WHCA examine the development of a main frame computer application for the National Security Council.

The purpose of this main frame application is to establish a classified document accountability system that can be used by the entire NSC staff.

NSC suggests an application design similar to the DOCLOG application currently existing in PROFS. At the same time, a FAAAS controlled access application should be developed and designed.

NSC points of contact will be Brian Merchant of the Secretariat (for the computer design) and James McCue of the Security Office (for the concept). If you have any questions and to discuss further application requirements, please contact one of them.

In order to assist the new administration in January 1989, early action on this request would be appreciated.

Thank you for your assistance in this matter.

March 18, 1988

MEMORANDUM FOR: GEORGE VAN ERON

FROM: JAMES T. McCUE

SUBJECT: Security Requirements for TOP SECRET and
Sensitive Compartmented Information
(SCI)

As you know, I am in the process of developing an NSC Security Regulation (NSC/SR). One of the areas I am looking at pertains to the procedures for receiving, dispatching, and maintaining accountability registers of TOP SECRET and SCI documents. I realize the NSC has a system of accountability and control for documents received at the NSC. I'm not sure that subject documents, handcarried into NSC offices, are placed into an accountability system. The question is: with instructional requirements imposed by the NSC/SR, can the system in place be used as is, or with minor modification, so that the "Purpose" of the NSC security program, as outlined below, can be accomplished?

I would appreciate your reviewing the following objectives and discussing with me the feasibility of this approach.

A. Purpose

1. To provide, within each NSC office, a central control system for TOP SECRET and CODEWORD documents.

2. To establish an inventory system for the identity, location, and disposition of TOP SECRET and CODEWORD material.

3. To enable the NSC to take timely downgrading/declassification of documents no longer requiring high level classification.

4. To assist in identification of TOP SECRET and CODEWORD documents which may be destroyed or retired.

B. Requirements

1. Each NSC Senior Director's office will have one terminal dedicated for data entry to ACTIVE DOCUMENTS.

2. One primary and one alternate, using the same password, will be authorized to access ACTIVE DOCUMENTS. One will be designated the TOP SECRET CONTROL OFFICER (TSCO); the other will be the ALTERNATE TSCO.

3. NSC offices will be able to access only their database.

4. Only the TSCO/ALTERNATE will be able to access their own DESTRUCTION RECORD and the TRANSFER OF DOCUMENTS RECORD.

5. The Director NSC Security Programs will have override capability for access to each database.

6. The ACTIVE DOCUMENTS database will be a permanent record system.

7. Documents in the DESTRUCTION RECORD and TRANSFER OF DOCUMENT database will remain in the system for one year after which they will be automatically dropped. Hard copy Destruction Certificates and Transfer Receipts will be retained for three years.

8. Quarterly printouts will be required for each NSC office so that they can conduct an inventory. Requirements will be established in an NSC Security Regulation to be published.

9. For purpose of audit trails, the system should include a query capability to trail a specific document, via its control number, from one database to another, without running a query of the entire database.

C. Database

CONTROL RECORD
FOR TOP SECRET DOCUMENTS
AND
COMPARTMENTED DOCUMENTS

ACTIVE DOCUMENTS

NSC Document Control Number _____
Originator's Document Control Number _____
Title of Document _____
Date of Document _____

Document is Number _____ of _____ copies
Number of Copies Received _____
Date Received in NSC Office _____
Agency That Issued the Document _____
Date Document to be Downgraded _____
Date Document to be Declassified _____
Classification of Title _____
Codeword(s) _____
NSC Action Officer _____
Document Stored in Security Container # _____
Disposition of Document: (Check One)
____ Transferred to Another NSC Office on _____
____ Transferred Outside the NSC on _____
Identity of Receiving Activity: _____

Receipt Number _____
Transferred to Destruction Record _____
Downgraded _____ Declassified _____

DESTRUCTION RECORD

NSC Control Number _____
Title of Document _____
Document Copy Number _____
Classification at Date of Destruction _____
NSC Official Authorizing Destruction:
Name _____
Title _____
Office _____
Method of Destruction _____
Destroyed By:
Destroying Official _____
Witnessing Official _____
Destruction Record Number _____
Destruction Record location _____

TRANSFER OF DOCUMENT

NSC Control Number _____
Title of Document _____
Document Copy Number _____
Classification of Document at Time of Transfer _____
Transferred to _____
NSC Official Authorizing Transfer _____
Name _____
Title _____
Office _____
Date of Transfer _____

Document Receipt Number _____
Documented Receipted For On _____
Document Receipt Locatation _____

~~CONFIDENTIAL~~

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

VAN

~~CONFIDENTIAL~~

5270

July 18, 1988

ACTION

MEMORANDUM FOR PAUL SCHOTT STEVENS

FROM: JAMES T. MCCUE *JTM*
SUBJECT: Classified Document Control Data Base

ISSUE

Definition of and requirements needed to establish a computer accountability system for Top Secret and SCI documents.

The purpose of this accountability system is to establish a computer registry within each NSC directorate for use by the office security manager (or alternate) and the NSC security office. Brian Merchant is responsible for the computer design.

OBJECTIVE

The Secretariat handles an estimated 80% of the Top Secret and codeword material received by NSC or sent by NSC. This material is already handled by an accountability system. The other 20% is not necessarily entered into a manual or automated accountability system. File copies of documents generated by the NSC may or may not be incorporated into our existing system. Working papers are generally not in any accountability system even though they may be kept in storage independently. Adoption of the proposed automated accountability system would enhance the total security environment of the NSC.

DISCUSSION

The possible options available to implement this requirement are:

- develop a mainframe computer application,
- develop a VAX computer application,
- develop a stand-alone application.

Each of these options have been examined and are discussed below. Unfortunately, there is no quick solution.

~~CONFIDENTIAL~~
Declassify on: OADR

DECLASSIFIED
PER NSC WAIVER, #2017-03
By VB NARA, Date 9/4/19

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CONFIDENTIAL

-2-

MAIN FRAME COMPUTER APPLICATION

This option would develop a computer accountability system on the WHCA/IBM main frame computer. Requirements would have to be developed for the design of software applications and the availability of modern technology.

Therefore, NSC should task White House Communications Agency (WHCA) to examine application requirements. Once approved by WHCA, the contractor would design a DOCLOG type file which would allow for document accountability tracking.

A parallel access file controlled by a FAAAS application would be designed at the same time.

VAX COMPUTER APPLICATION

Discussions were held with WHSSS. They do not have the resources available to develop this application. In addition, the hardware support requires a LAN configuration across the entire staff to implement.

STAND-ALONE APPLICATION

DBase III was a possible stand-alone application. However, after discussions with IBM, DBase III does not look feasible because:

- it has very limited capability and is designed for use by one or two users,
- while it allows software design by the user, the resultant software package is not as versatile as that of a main frame application.

Concurrence: George Van Eron

RECOMMENDATION

That you sign the memorandum to Pat McGovern at Tab I.

_____ Approve

_____ Disapprove

Attachment

Tab I - Memorandum to Pat McGovern

Prepared by:
Brian T. Merchant

CONFIDENTIAL

~~CONFIDENTIAL~~

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

5270

MEMORANDUM FOR COLONEL PATRICK MCGOVERN
WHITE HOUSE COMMUNICATIONS AGENCY

FROM: PAUL SCHOTT STEVENS
SUBJECT: Document Accountability System

It is requested that WHCA examine the development of a main frame computer application for the National Security Council.

The purpose of this main frame application is to establish a classified document accountability system that can be used by the entire NSC staff.

NSC suggests an application design similar to the DOCLOG application currently existing in PROFS. At the same time, a FAAAS controlled access application should be developed and designed.

NSC points of contact will be Brian Merchant of the Secretariat (for the computer design) and James McCue of the Security Office (for the concept). If you have any questions and to discuss further application requirements, please contact one of them.

In order to assist the new administration in January 1989, early action on this request would be appreciated.

Thank you for your assistance in this matter.

National Security Council
The White House

C7

30 JUL 20 P 1: 14

System # _____
Package # 5270
DOCLOG C7 A/O _____

	SEQUENCE TO	HAS SEEN	DISPOSITION
Bob Perito	<u>1</u>	<u>RmP</u>	<u>A</u>
Marybel Batjer			
Paul Stevens	<u>2</u>	<u>✓</u>	
John Negroponte			
Colin Powell			
Paul Stevens			
Situation Room			
West Wing Desk	<u>3/</u>	<u>TC</u>	<u>✓</u>
NSC Secretariat	<u>4</u>		<u>N</u>

I = Information A = Action R = Retain D = Dispatch N = No further Action

PKC-

NSC/S;

UFAR per Stevens.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

May 3, 1988

MEMORANDUM FOR **GEORGE VAN ERON**

NANCY V. MENAN
JAMES T. McCUE
BRIAN T. MERCHANT
GARY MOORE
MARY A. DIX

FROM: NICHOLAS ROSTOW *NR*.

SUBJECT: Personnel Security Programs

Attached at Tab I is a General Accounting Office survey that seeks information regarding the NSC's information and personnel security programs. Please review the survey and answer those questions that involve information in the possession of your directorate or matters for which your directorate is responsible. It appears to me that the Administrative Office should answer questions 1 and 2. The Office of Information Security and Policy Review should answer questions 10, 11, 12, 13, 14, 24, 25, 26 and 27. Finally, our Security Office should answer questions 2-9, 15-23, and 28-39. Gary Moore and Brian Merchant should provide input to the Security Office for questions that involve special access programs.

You should annotate with an "E" answers that are estimates. If you have questions regarding the survey, please contact Jonathan Scharfen at extension 5026. He will, in any event, be in touch with you regarding the survey.

If possible, please provide your answers to this office by Thursday, May 12.

Thank you.

Attachment

Tab I - General Accounting Office Survey

TAB

I

United States Senate

WASHINGTON, D.C. 20510

April 19, 1988

The Honorable Paul Schott Stevens
Executive Secretary
National Security Council
The White House
Washington, D.C. 20500

Dear Mr. Stevens:

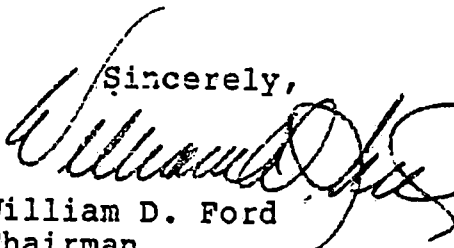
Since 1984, the General Accounting Office, at the request of the Committees on Government Operations and Post Office and Civil Service, has conducted several surveys of the government's information and personnel security programs. Their last survey covered calendar years 1984 and 1985. We have requested the General Accounting Office to obtain updated and additional information relative to calendar years 1986 and 1987. We would appreciate your response to the enclosed questionnaire by May 16, 1988.

Thank you very much for your prompt attention to this request.

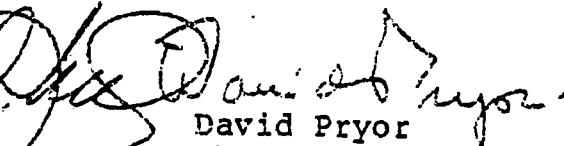
Sincerely,



Jack Brooks
Chairman
Committee on
Government Operations



William D. Ford
Chairman
Committee on Post Office
and Civil Service



David Pryor
Chairman
Subcommittee on
Federal Services,
Post Office and
Civil Service

REQUEST FOR INFORMATION RELATIVE TO
INFORMATION AND PERSONNEL SECURITY

Introduction:

Throughout this questionnaire, we are talking about the number of people; for that reason, the number of positions should not be converted to full-time equivalents.

When an estimate is given for any answer, please precede the estimated number with the letter "E".

Unless otherwise specified, the requested information should be as of December 31, 1986, and December 31, 1987.

Please be specific when indicating whether an answer is classified.

If your agency participates in the Defense Industrial Security Program (DISP), you need not provide data on those contractor employees covered by the program, because such data will be obtained directly from the Department of Defense. If you also have contractor employees not covered by the DISP, please provide the requested data for them.

If any information will not be obtainable within the specified timeframe, please send that information which is available and indicate a date by which we may expect the remainder.

If you have any questions, please call Mr. Don Lentz 275-4052 or Mr. Irv Boker, 275-3973. Please return the completed questionnaire by May 16, 1988, to:

Mr. Irv Boker, Room 4100
U.S. General Accounting Office
Washington, D.C. 20548

QUESTIONNAIRE

GENERAL

1. Approximately how many people were employed by your agency as of December 31, 1986, and December 31, 1987? (The total should include both full- and part-time employees. If the exact number is not available, please give your agency's best estimate, and indicate such by preceding the number with the letter "E").

	<u>1986</u>	<u>1987</u>
Employees	_____	_____

SECURITY CLEARANCES

2. As of December 31, 1986, and December 31, 1987, approximately how many of your employees and how many employees of your contractors were cleared for access to classified information? Please count the individuals based on their highest level of clearance. (If the exact number is not known, please give your agency's best estimate. Do not include contractor employees who were granted clearances by the Defense Investigative Service. Enter the number on each line. If none, enter "0").

	<u>1986</u>		<u>1987</u>	
<u>Highest Level of Clearance</u>	<u>Agency Employees</u>	<u>Contractor Employees</u>	<u>Agency Employees</u>	<u>Contractor Employees</u>
TOP SECRET	_____	_____	_____	_____
SECRET	_____	_____	_____	_____
CONFIDENTIAL	_____	_____	_____	_____

3. How many SCI and non-SCI special access programs did your agency have at the close of calendar years 1986 and 1987? How many billets were authorized for these programs and how many agency and contractor employees were granted special access authorizations for them for each of those years? (If the exact number is not available, please give your agency's best estimate, and indicate such by preceding the number with the letter "E").

	<u>1986</u>		<u>1987</u>	
	<u>SCI</u>	<u>Non-SCI</u>	<u>SCI</u>	<u>Non-SCI</u>
Programs	_____	_____	_____	_____
Billets	_____	_____	_____	_____
Agency employees	_____	_____	_____	_____
Contractor employees	_____	_____	_____	_____

4. How many personnel security clearances, SCI accesses, and non-SCI special access program (SAP) accesses did you grant (or were granted) to your employees and employees of your contractors during calendar years 1986 and 1987? (If the exact number is not available, please give your agency's best estimate and indicate such by preceding the number with the letter "E". Do not include clearances granted to contractor employees by the Defense Investigative Service.)

	<u>1986</u>		<u>1987</u>	
	<u>Agency</u>	<u>Contractor</u>	<u>Agency</u>	<u>Contractor</u>
TOP SECRET	_____	_____	_____	_____
SECRET	_____	_____	_____	_____
CONFIDENTIAL	_____	_____	_____	_____
TOTAL	_____	_____	_____	_____
SCI Access	_____	_____	_____	_____
Non-SCI Special Access Program	_____	_____	_____	_____

5. How many requests for security clearances and SCI and non-SCI SAP accesses were in process (incomplete National Agency Checks, Background Investigations, adjudications, etc.) at the end of calendar years 1986 and 1987? (If the exact number is not available, please give your agency's best estimate, and indicate such by preceding the number with the letter "E").

Level of Request
for Clearance and
Access in Process

	<u>1986</u>		<u>1987</u>	
	<u>Agency</u>	<u>Contractor</u>	<u>Agency</u>	<u>Contractor</u>
TOP SECRET	_____	_____	_____	_____
SECRET	_____	_____	_____	_____
CONFIDENTIAL	_____	_____	_____	_____
TOTAL	_____	_____	_____	_____
SCI Access	_____	_____	_____	_____
Non-SCI SAP Access	_____	_____	_____	_____

6. What was the average time (in calendar days) required for you or another agency to complete the investigative work incident to the granting of a top secret and secret security clearance and SCI and non-SCI SAP access during calendar years 1986 and 1987? (Do not include the time involved in the preparation and internal processing of the personnel security questionnaire and in the subsequent adjudicative process. Include, if appropriate, the average time taken by the Defense Investigative Service to process your requests for clearances for contractor employees.)

<u>Level of Clearance</u>	<u>1986</u>		<u>1987</u>	
	<u>Agency</u>	<u>Contractor</u>	<u>Agency</u>	<u>Contractor</u>
TOP SECRET	_____	_____	_____	_____
SECRET	_____	_____	_____	_____
CONFIDENTIAL	_____	_____	_____	_____
SCI Access	_____	_____	_____	_____
Non-SCI SAP Access	_____	_____	_____	_____

7. How many requests for your employees and employees of your contractors for security clearances and SCI and non-SCI SAP access were denied during calendar years 1986 and 1987? How many clearances and SCI and non-SCI accesses were revoked for reasons of risk or potential risk to national security or administratively because of insufficient need? Identify, by placing in brackets, those requests for clearances or revocations for contractor employees administered by the Defense Investigative Service. (If the exact number is not available, please give your agency's best estimate, and indicate such by preceding the number with the letter "E").

<u>Agency</u> <u>1986</u>	<u>Level of Clearance and Access</u>					<u>Total</u>
	<u>Top Secret</u>	<u>Secret</u>	<u>Confidential</u>	<u>SCI access</u>	<u>Non-SCI SAP access</u>	
Number of Denials	_____	_____	_____	_____	_____	_____
Revocations-Because of: Risk or Potential Risk	_____	_____	_____	_____	_____	_____
Administrative-No Further Need	_____	_____	_____	_____	_____	_____
Total Number of Revocations	_____	_____	_____	_____	_____	_____
<u>1987</u>						
Number of Denials	_____	_____	_____	_____	_____	_____
Revocations-Because of: Risk or Potential Risk	_____	_____	_____	_____	_____	_____
Administrative-No Further Need	_____	_____	_____	_____	_____	_____
Total Number of Revocations	_____	_____	_____	_____	_____	_____

<u>Contractor</u> <u>1986</u>	<u>Top</u> <u>Secret</u>	<u>Secret</u>	<u>Confi-</u> <u>dential</u>	<u>SCI</u> <u>access</u>	<u>Non-SCI</u> <u>SAP access</u>	<u>Total</u>
Number of Denials	_____	_____	_____	_____	_____	_____
Revocations-Because of: Risk or Potential Risk	_____	_____	_____	_____	_____	_____
Administrative-No Further Need	_____	_____	_____	_____	_____	_____
Total Number of Revocations	_____	_____	_____	_____	_____	_____
<u>1987</u>						
Number of Denials	_____	_____	_____	_____	_____	_____
Revocations-Because of: Risk or Potential Risk	_____	_____	_____	_____	_____	_____
Administrative-No Further Need	_____	_____	_____	_____	_____	_____
Total Number of Revocations	_____	_____	_____	_____	_____	_____

6. Please provide copies of your agency's policies and procedures governing the periodic reinvestigation of individuals after the initial granting of clearances and SCI access. How many completed reinvestigations of any type did your agency conduct or have conducted for it during calendar years 1986 and 1987? What was the average time (in calendar days) required for completion of the reinvestigation? (If the exact number is not available, please give your agency's best estimate, and indicate such by preceding the number with the letter "E").

	<u>Level of Clearance and Access</u>					
<u>1986</u>	<u>Top</u> <u>Secret</u>	<u>Secret</u>	<u>Confi-</u> <u>dential</u>	<u>SCI</u> <u>access</u>	<u>Non-SCI</u> <u>SAP access</u>	<u>Total</u>
Number of completed Reinvestigations:						
Agency	_____	_____	_____	_____	_____	_____
Contractor	_____	_____	_____	_____	_____	_____
Average Time Required:						
Agency	_____	_____	_____	_____	_____	_____
Contractor	_____	_____	_____	_____	_____	_____

<u>1987</u>	<u>Level of Clearance and Access</u>					<u>Total</u>
	<u>Top Secret</u>	<u>Secret</u>	<u>Confidential</u>	<u>SCI access</u>	<u>Non-SCI SAP access</u>	
Number of completed Reinvestigations:						
Agency	_____	_____	_____	_____	_____	_____
Contractor	_____	_____	_____	_____	_____	_____
Average Time Required:						
Agency	_____	_____	_____	_____	_____	_____
Contractor	_____	_____	_____	_____	_____	_____

9. Approximately how much did you spend in calendar years 1986 and 1987 for security clearance investigations, reinvestigations, special investigations, and adjudications, including inhouse costs, reimbursements to other federal agencies, and contract costs? Please identify specific costs if possible (i.e. adjudicative costs, Defense Investigative Service vs. Office of Personnel Management, etc.).

<u>Inhouse costs</u>	<u>1986</u>	<u>1987</u>
_____	_____	_____
_____	_____	_____
_____	_____	_____
Total	_____	_____
<u>Reimbursement to other agencies</u>		
_____	_____	_____
_____	_____	_____
_____	_____	_____
Total	_____	_____
<u>Contracted investigative services</u>		
_____	_____	_____
_____	_____	_____
_____	_____	_____
Total	_____	_____

CLASSIFICATION MANAGEMENT

10. How many employees of your agency were authorized to classify information (either original or derivative authority) at the top secret level and below and at the secret level and below as of December 31, 1986, and December 31, 1987? Please count the individuals based on their highest level of authority. (if the exact number is not known, please give your agency's best estimate, and indicate such by preceding the number with the letter "E").

Level of Information
Classified

Agency
Classifiers

	<u>1986</u>		<u>1987</u>	
	<u>Original</u> <u>Authority</u>	<u>Derivative</u> <u>Authority</u>	<u>Original</u> <u>Authority</u>	<u>Derivative</u> <u>Authority</u>
TOP SECRET and below	_____	_____	_____	_____
SECRET and below	_____	_____	_____	_____

11. Does your agency require its classifiers to be certified? Does your agency require training for classifiers? If you answer yes, please provide the requirements of the certification and syllabus of the training requirements.

Certification
of Classifiers

Training Required
for Classifiers

_____ yes

_____ yes

_____ no

_____ no

12. Does your agency use classification guides? If you answer yes, how many were issued as of December 31, 1986, and December 31, 1987?

Classification
Guides Used

Number of Classification
Guides Issued as of

_____ yes

December 31, 1986

December 31, 1987

_____ no

ACCESS BY HISTORIANS AND FORMER PRESIDENTIAL APPOINTEES

Section 4.3 of Executive Order 12356 authorizes access to classified information by historical researchers and former presidential appointees. Please provide the following information on the number of individuals given such access.

<u>1986</u>	<u>Historical Researchers</u>	<u>Former Presidential Appointees</u>
Number of individuals granted access during calendar year 1986	_____	_____
Number of individuals denied access during calendar year 1986	_____	_____
Number of individuals with access as of December 31, 1986	_____	_____

<u>1987</u>	<u>Historical Researchers</u>	<u>Former Presidential Appointees</u>
Number of individuals granted access during calendar year 1987	_____	_____
Number of individuals denied access during calendar year 1987	_____	_____
Number of individuals with access as of December 31, 1987	_____	_____

14. Please provide a copy of your agency's procedures governing section 4.3 of the executive order. If your procedures do not include a provision for this section of the order, please identify the position of the individual authorized to grant access to historical researchers and former presidential appointees.

NONDISCLOSURE AGREEMENTS

15. As of December 31, 1986, and December 31, 1987, how many employees of your agency and employees of your contractors had signed a Standard Form (SF) 189, SF 189-A, Form 4193, DD Form 1847-1 (for SCI access), or other nondisclosure agreement? (Please attach copies of agreements other than SF 189, SF 189-A, Form 4193 and DD Form 1847-1.)

<u>1986</u>	<u>Agency Employees</u>	<u>Contractor Employees</u>
SF 189	_____	_____
SF 189-A	_____	_____
Form 4193	_____	_____
DD Form 1847-1	_____	_____
_____ (other)	_____	_____
_____ (other)	_____	_____
 <u>1987</u>	 <u>Agency Employees</u>	 <u>Contractor Employees</u>
SF 189	_____	_____
SF 189-A	_____	_____
Form 4193	_____	_____
DD Form 1847-1	_____	_____
_____ (other)	_____	_____
_____ (other)	_____	_____

16. Has your agency issued written procedures for use of the SF 189 and 189-A?

____ Yes ____ No

If you answered "yes", please provide a copy of the procedures.

17. Information Security Oversight Office (ISOO) instructions on the use of SF 189 and SF 189-A did not designate a date for completing implementation for individuals who already had access to classified information. What date or dates did you establish for obtaining a signed SF 189 or SF 189-A from every individual granted access to classified information prior to the December 29, 1987, letter from ISOO directing immediate suspension of the program?

	<u>SF 189</u>	<u>SF 189-A</u>
None	_____	_____
Date	_____	_____

18. Did you require all of your employees and all of your contractors' employees to sign either an SF 189 or SF 189-A?

_____ Yes

_____ No

If you answered "no", which employees were not required to sign an SF 189 or SF 189-A?

19. What means of enforcement did you have to ensure that all required individuals signed an SF 189 or SF 189-A? (Please explain.)

20. When do you require individuals--new employees, newly cleared employees, and employees who already have access to classified information--to sign the nondisclosure agreements (SF 189, SF 189-A, Form 4193, DD Form 1847-1, and others)? (Please check the appropriate line or lines.)

<u>New employees</u>	<u>SF 189</u>	<u>SF 189-A</u>	<u>Form 4193</u>	<u>DD Form 1847-1</u>	<u>Other</u>
When hired	_____	_____	_____	_____	_____
When a clearance is requested	_____	_____	_____	_____	_____
When a clearance is granted	_____	_____	_____	_____	_____
After a security briefing	_____	_____	_____	_____	_____
Before access to classified data	_____	_____	_____	_____	_____
Other (please explain on attachment)	_____	_____	_____	_____	_____

Newly cleared employees

	<u>SF 189</u>	<u>SF 189-A</u>	<u>Form 4193</u>	<u>DD Form 1847-1</u>	<u>Other</u>
After a security briefing	_____	_____	_____	_____	_____
Before access to classified data	_____	_____	_____	_____	_____
Other (please explain on attachment)	_____	_____	_____	_____	_____

Employees already having access

	<u>SF 189</u>	<u>SF 189-A</u>	<u>Form 4193</u>	<u>DD Form 1847-1</u>	<u>Other</u>
All employees have signed agreements	_____	_____	_____	_____	_____
After a security briefing	_____	_____	_____	_____	_____
Before access to classified data	_____	_____	_____	_____	_____
Other (please explain on (attachment)	_____	_____	_____	_____	_____

21. How many employees of your agency and contractors had refused to sign the SF 189 SF 189-A, Form 4193, DD Form 1847-1, or other nondisclosure agreement as of December 31, 1987?

	<u>Agency Employees</u>	<u>Contractor Employees</u>
SF 189	_____	_____
SF 189-A	_____	_____
Form 4193	_____	_____
DD Form 1847-1	_____	_____
Other	_____	_____

22. What action has been taken with respect to those individuals who refused to sign the SF 189, SF 189-A, Form 4193, DD Form 1847-1, or other nondisclosure agreement? Please indicate the number of employees involved and indicate the action or actions taken. For example, if any employee's security clearance was suspended and the individual was also reassigned to another position, the individual would be included in two of the categories described below.

	<u>Agency Employees</u>	<u>Contractor Employees</u>
Security clearance suspended	_____	_____
Security clearance revoked	_____	_____
No action taken on clearance	_____	_____
Individual reassigned to another position or duties with:		
No reduction in salary	_____	_____
Reduction in salary	_____	_____
Individual resigned	_____	_____
Individual's employment terminated	_____	_____
Case still under consideration	_____	_____
Other administrative sanctions (please describe below)	_____	_____

23. How many SF 189, SF 189-A, Form 4193, DD Form 1847-1, or other nondisclosure agreements were signed by employees of your agency and contractors during the periods of December 22, 1987 (date of enactment of on the use of nondisclosure) through March 31, 1988?

<u>December 22, 1987 - March 31, 1988</u>	<u>Agency Employees</u>	<u>Contractor Employees</u>
SF 189	_____	_____
SF 189-A	_____	_____
Form 4193	_____	_____
DD Form 1847-1	_____	_____
<u>(Other)</u>	_____	_____
<u>(Other)</u>	_____	_____
Total	_____	_____

PRE-PUBLICATION REVIEW AND UNAUTHORIZED DISCLOSURES

4. Are any of your agency's employees required to submit to any pre-publication review procedure (other than to review official statements on behalf of the agency)?

_____ Yes

_____ No (Please skip to Question 28)

25. Approximately how many books, articles, speeches, and other materials, by category, were reviewed during your agency's pre-publication review process (described in Question 24) for calendar years 1986 and 1987? If possible, identify the reason for pre-publication review. If the number is not known, please give your agency's best estimate (required by regulation or nondisclosure agreement). Please enter the number on each line. (If none, enter "0".)

Reason for Pre-Publication Review	Type of Material			
	<u>Books</u>	<u>Articles</u>	<u>Speeches</u>	<u>Other (Please Specify)</u>
<u>1986</u>				
Regulation	_____	_____	_____	_____
SCI Agreement	_____	_____	_____	_____
Non-SCI SAP Agreement	_____	_____	_____	_____
Other (please specify)	_____	_____	_____	_____
<u>1987</u>				
Regulation	_____	_____	_____	_____
SCI Agreement	_____	_____	_____	_____
Non-SCI SAP Agreement	_____	_____	_____	_____
Other (please specify)	_____	_____	_____	_____

26. Please estimate the average number of working days that elapse from the date of receipt of a request for pre-publication review of each type of document below, to the date the requestor is informed of the final results. If you have not had experience in reviewing a type of document, enter "NA" on the applicable line. (Enter estimated average number of working days on each line).

Estimated Average Working Days

_____ Books	_____ Articles
_____ Speeches	_____ Other (please specify)
_____	_____

27. During calendar years 1986 and 1987, approximately how many employees were assigned, and working days were used for pre-publication review as described in Question 24?

	<u>1986</u>	<u>1987</u>
Estimated number of employees assigned	_____	_____
Estimated number of working days used	_____	_____

28. During calendar years 1986 and 1987, did your agency experience any unauthorized disclosures of classified information? (Check one).

	<u>1986</u>	<u>1987</u>
Yes	_____	_____
No (Please skip to Question 32)	_____	_____

29. For calendar years 1986 and 1987, please indicate the total number of unauthorized disclosures, the number of unauthorized disclosures made through books, articles, speeches, written or given by then-current and former employees, the number which were not reported to the Department of Justice, and the number made by individuals who had previously signed a nondisclosure agreement.

	<u>1986</u>	<u>1987</u>
Total number of known unauthorized disclosures	_____	_____
Number not reported to Department of Justice	_____	_____
Number made through published writing or speeches by: then-current employees, or	_____	_____
Former employees	_____	_____
Number made by individuals who had previously signed a nondisclosure agreement	_____	_____

30. How many unauthorized disclosures were investigated by your agency or referred to another agency for investigation during calendar years 1986 and 1987?

	<u>1986</u>	<u>1987</u>
Number of cases investigated by your agency	_____	_____
Number of cases referred to another agency for investigation, after your investigation was completed	_____	_____

Number of cases referred to another agency for investigation, that your agency did not investigate.

1986

1987

31. How many employees of your agency and employees of your contractors were denied further access to classified information, because of their unwillingness to cooperate with the investigation of an unauthorized disclosure (because the use of the polygraph was involved or for other reasons), during calendar years 1986 and 1987? How many were subjected to other administrative sanctions?

<u>Employees denied further access to classified information</u>	<u>1986</u>		<u>1987</u>	
	<u>Polygraph Involved</u>	<u>Other Reasons</u>	<u>Polygraph Involved</u>	<u>Other Reasons</u>
Agency	_____	_____	_____	_____
Contractor	_____	_____	_____	_____
<u>Employees subjected to other administrative sanctions</u>				
Agency	_____	_____	_____	_____
Contractor	_____	_____	_____	_____

2. Please indicate which of your agency's policies and procedures governing contacts between your employees and media representatives are for national security reasons. Also, explain or provide documentation explaining the method by which your agency assures that all employees with security clearances are apprised of these policies and procedures.

POLYGRAPH ACTIVITY

33. Did your agency employ polygraph operators during calendar years 1986 and 1987?

	<u>1986</u>	<u>1987</u>
Yes	_____	_____
No	_____	_____

34. As of December 31, 1986, and December 31, 1987, how many polygraph operators were employed by your agency? How many contracts for polygraph examinations did you have?

	<u>1986</u>	<u>1987</u>
Agency employees	_____	_____
Number of contracts	_____	_____

35. Do you have plans to employ any additional polygraph operators or contract out for services? If so, why and how many?

_____ Agency employees

_____ Contractors

36. As of December 31, 1986 and December 31, 1987, how many polygraph machines, if any, did your agency possess? How many were procured during calendar years 1986 and 1987? Do you have plans to procure any additional polygraph machines, and if so, how many?

	<u>1986</u>	<u>1987</u>
Number of polygraph machines on hand at end of the year	_____	_____
Number of polygraph machines procured during the year	_____	_____
Plans to procure additional polygraph machine		
_____ yes (number of machines _____)		
_____ no		

37. Approximately how many polygraph tests were conducted of your employees or applicants for employment by, or for, your agency? Please list by the indicated categories for each of the listed calendar years. If they were conducted by another agency or contractor, so indicate. Identify how many tests resulted in security clearance action (denial, revocation, suspension, other) and explain.

Reason for Polygraph Test

	<u>1986</u>		<u>1987</u>	
<u>Criminal or specific incident investigations</u>	<u>Number of Tests</u>	<u>Clearance Action</u>	<u>Number of Tests</u>	<u>Clearance Action</u>
Conducted by agency	_____	_____	_____	_____
Conducted by other agencies or contractors (list)	_____	_____	_____	_____
<u>Pre-employment screening</u>				
Conducted by agency	_____	_____	_____	_____
Conducted by other agencies or contractors (list)	_____	_____	_____	_____
<u>Pre-access screening</u>				
Conducted by agency	_____	_____	_____	_____
Conducted by other agencies or contractors (list)	_____	_____	_____	_____
<u>Subsequent screening</u>				
Conducted by agency	_____	_____	_____	_____
Conducted by other agencies or contractors (list)	_____	_____	_____	_____
Other (explain)	_____	_____	_____	_____
Conducted by agency	_____	_____	_____	_____
Conducted by other agencies or contractors (list)	_____	_____	_____	_____
Total (do not double count)	_____	_____	_____	_____
<u>Summary</u>				
Conducted by agency	_____	_____	_____	_____
Conducted by other agencies or contractors (list)	_____	_____	_____	_____
Total (should be the same number as in above "total")	_____	_____	_____	_____

Explanation of Clearance Actions:

38. Under what authority, regulations and rules are your polygraph examinations conducted? Please list citations and attach copies. Highlight any changes since 1985. Also, indicate any plans to revise these governing regulations proposed at this time. Please describe the changes and attach copies of these proposals, if available. In particular, describe which employees, and indicate how many, would be potentially covered under each type of polygraph examination (specific incident investigation, screening or other uses (described) and the projected number of exams to be given in each category.

39. Please provide the qualifications required of individuals employed as polygraph examiners by your agency.

40. Please enter below the name, title, and telephone number of the person to be contacted if clarification or additional information is needed:

Agency: _____

Name: _____

Title: _____

Location: _____

Telephone number: (Area Code) _____ (Number) _____

If you have any questions, please contact either GAO staff member:
Mr. Don Lentz, 275-4052 or Mr. Irv Boker, 275-3973

Thank you for your time. Please return the completed questionnaire by
May 16, 1988, to:

Mr. Irv Boker, Room 4100
U.S. General Accounting Office
Washington, D.C. 20548

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

March 24, 1988

MEMORANDUM FOR GEORGE VAN ERON
✓ MARY DIX

FROM: JAMES T. MCCUE

SUBJECT: Security Approval Required for
Entry-on-Duty

Reference is made to Paul's memorandum of March 22, 1988, above subject and to Mary's prof note of March 23, 1988, subject: "Paul's Memo."

Attached is a draft of a proposed chapter to the NSC Security Regulation I have been working on. The main thrust of the draft allows us two options not in use in the NSC. They are:

1. Procedures for Interim TOP SECRET clearances, — *see para 11.2.*
and
2. Utilization of the "Compelling Need" authority which will permit eligible personnel access to SCI provided they have a valid, though outdated, Background Investigation and a final TOP SECRET clearance.

Under present procedures, people enter-on-duty in the NSC without a system established for ensuring that they are effectively denied access to information for which they have not been cleared and/or indoctrinated.

With your help, I hope to establish a system similiar to that existing in the rest of the Executive Branch.?

I would appreciate your reviewing the attached draft. We can then meet to discuss it or, if you prefer, provide me with your ideas so that we can develop a proposal which will meet Paul's objectives.

Section II, Security Clearances

9. General

a. Only United States citizens shall be granted a personnel security clearance and indoctrinated for access to Sensitive Compartmented Information (SCI). All candidates for duty with the NSC, be they military or civilian permanent staff, detailees, consultants or contractors, must have a TOP SECRET (TS) security clearance and meet the eligibility requirements for access to SCI. *sk*

b. A candidate who has been selected for a position with the NSC and does not have an existing TS security clearance or recent Background Investigation (BI) will be subject to an investigation. The length of time it takes to complete any required investigation cannot be predetermined. Although existing collateral security clearances are generally transferable between agencies of the Executive Branch; SCI authorizations are not. Selectees without a prior security clearance or qualifying recent background investigation require a full BI update. *what happened to the agreement between the WH and the FBI, which indicates a 60-day turn around for initial investigations (60-day turn around confirmed by the FBI.)*

c. Selectees shall not be employed in a Sensitive Compartmented Information Facility (SCIF) until they have been indoctrinated for SCI. The reason for this prohibition is that SCIFs in the NSC contain secure voice communication systems in addition to SCI material in their ADP systems, in security cabinets and, in most cases, in daily use within the work areas. Due to the complexity of security measures to preclude unauthorized access, only SCI indoctrinated personnel shall be assigned to work in a SCIF. *This paragraph says we will not employ someone until he/she has SCI access.*

who is this?
d. The D/NSCSP shall provide the Director for Administration with a written notification of the security clearance and SCI authorization status of the selectee. The notification shall stipulate any prohibition against entry-on-duty pending completion of security clearance determinations and SCI authorizations associated with duty in the NSC. Should the selecting NSC Senior Director determine that the procedures outlined in paragraph 10, below, will cause an undue delay and that it is in the national interest to permit the selectee to enter-on-duty pending completion of the requisite BI or SCI eligibility determination, the NSC *This paragraph says we can employ someone without SCI access, if certain actions are taken.*

Senior Director may take the action required in paragraph 11 a. or b., below, as appropriate.

10. Application for a TOP SECRET Security Clearance and Access to Sensitive Compartmented Information (SCI)

a. TOP SECRET Security Clearance. A promising candidate for a position in the NSC must complete an Standard Form 86 (Security Investigation Data for Sensitive Position) (SF 86) before being interviewed by the D/NSCSP. The interview addresses questions asked on the SF 86 and is designed to elicit information which will assist management in the selection process. The Executive Director, NSC will be advised by the D/NSCSP of any issues arising from the interview which could possibly result in denial of a TOP SECRET clearance or SCI indoctrination. If required, additional security forms will be furnished to the selectee by the D/NSCSP.

I thought this was changed.

b. SCI Processing. Access to SCI is granted by the following consecutive steps:

(1). a determination by the NSC Senior Director that the position to be occupied by the selectee requires access to SCI ("need-to-know" determination);

All NSC positions require SCI.

(2). the selectee must have been the subject of a completed BI covering the most recent fifteen years of his or her life. A BI which meets these requirements, and is not more than five years old, will generally satisfy requirements for SCI indoctrination;

(3). a TOP SECRET security clearance must have been issued, or certified to, by the D/NSCSP;

(4). approval must be received from the CIA for SCI indoctrination; and

(5). indoctrination must be completed before access to SCI is authorized.

OK

c. On receipt of notification from the CIA that the selectee has been indoctrinated for SCI, the D/NSCSP will send a written notification to the NSC Senior Director in whose office the selectee is assigned.

OK

11. Exceptions to Investigative Requirements.

In exceptional cases, where a selectee has a BI more than five years old and has been continuously employed in the Executive Branch since his or her most recent qualifying BI, an NSC Senior Director may determine it is necessary or advisable in the national interest to request the D/NSCSP to grant the selectee an Interim TOP SECRET (ITS) security clearance or, if the selectee has a TS clearance but requires a current BI to

Should we have a form request for both an ITS and "Compelling Need", that the Sr. Dir. can sign?

What does this include?

qualify for SCI indoctrination, to request access to SCI due to a "Compelling Need". An ITS clearance is not valid for access to SCI. The NSC Senior Director may take one of the following actions:

a. Request for Interim TOP SECRET. A

Senior Director may opt to request the selectee be granted an ITS clearance pending completion of the required investigation. The NSC Senior Director shall submit a written request to the D/NSCSP justifying the need for the ITS. Consideration will be given such request provided the selectee has been the subject of a current favorable National Agency Check and a new BI has been initiated.

Because the granting of an ITS clearance does not qualify a selectee for eligibility for access to SCI, this option does not apply to a selectee who is to be assigned to an area accredited by the United States Secret Service as a Sensitive Compartmented Facility (SCIF) in which SCI material is openly stored (see paragraph 2. ae). Prior to permitting a selectee to enter-on-duty with an ITS clearance, the NSC Senior Director shall develop a security plan designed to ensure that the selectee is denied access to SCI in a closed storage SCIF (see paragraph 2. i). The security plan shall address the following actions:

(1). procedures to deny the selectee access to the cipher system code for controlling entry to the SCIF;

(2). procedures to deny the selectee access and lock combinations to security cabinets containing SCI;

(3). procedures to deny the selectee access and passwords to computers which contain SCI material;

(4). procedures to deny the selectee access to secure voice communications;

(5). procedures to ensure that, while in the SCIF, the selectee is under continuous escort by an SCI indoctrinated co-worker, and

(6). procedures for ensuring that the selectee will not receive SCI material via the mail distribution system or messenger system.

b. "Compelling Need" Request for Access to SCI

Selectees who have a final TS certified to/by the D/NSCSP but require an updated BI for SCI indoctrination eligibility, may be eligible for early SCI indoctrination based on a justified "compelling need" established by the selecting NSC Senior Director. Under this option, once the NSC Senior Director has made his or her determination of the necessity for early access to SCI, he or she may submit a memorandum to the D/NSCSP, subject: "Compelling Need Request for Access to

After saying an ITS can be granted, this sentence indicates that for NSC personnel, this will not be possible.

Same issue. Sr. Dir. develop their own plan?

This means someone can answer the phones, as long as a cleared person is present. He/she may do nothing else.

OK

SCI by (name of employee)". The request shall include the selectee's:

- (1). full name;
- (2). date and place of birth;
- (3). Social Security Account Number, rank/grade, and, if active duty military, branch of service;

(4). duty title and SCI accesses required;

(5). justification establishing the immediate need for access to SCI and an explanation as to why another indoctrinated passholder cannot perform the SCI related task until the passholder is granted SCI access through the normal process.

We don't have extra bodies floating around looking to do other people's jobs.

c. On receipt of the information required in d., above, the D/NSCSP will enclose the request with a formal request to the CIA. The latter request will include a copy of the passholder's most recent SF 86.

ok

d. Passholder's with SCI access are subject to a periodic reinvestigation every five years.

11. Consultants

Consultants are subject to the same investigative requirements as passholders if they require access to TOP SECRET or SCI information. Once a prospective consultant has been tentatively approved for appointment, the D/NSCSP should be notified in order that expeditious action may be taken to identify and confirm existing clearances or to initiate any investigations considered appropriate for the level of access required.

ok

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

March 24, 1988

MEMORANDUM FOR [✓]GEORGE VAN ERON
MARY DIX

FROM: JAMES T. MCCUE *Jm*

SUBJECT: Security Approval Required for
Entry-on-Duty

Reference is made to Paul's memorandum of March 22, 1988, above subject and to Mary's prof note of March 23, 1988, subject: "Paul's Memo."

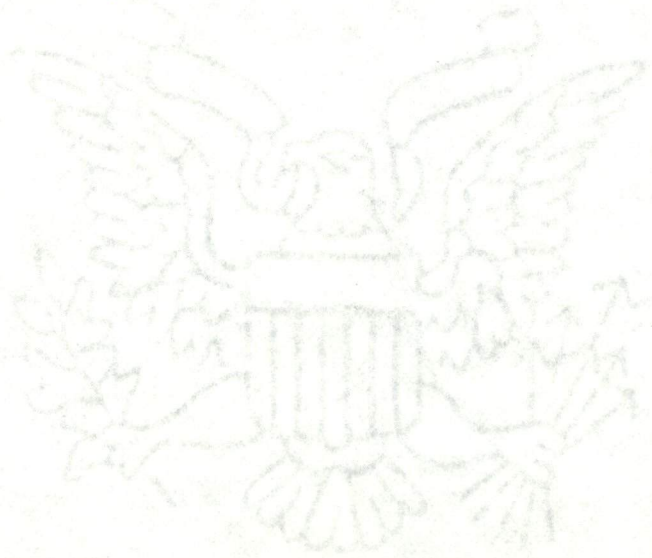
Attached is a draft of a proposed chapter to the NSC Security Regulation I have been working on. The main thrust of the draft allows us two options not in use in the NSC. They are:

1. Procedures for Interim TOP SECRET clearances, and
2. Utilization of the "Compelling Need" authority which will permit eligible personnel access to SCI provided they have a valid, though outdated, Background Investigation and a final TOP SECRET clearance.

Under present procedures, people enter-on-duty in the NSC without a system established for ensuring that they are effectively denied access to information for which they have not been cleared and/or indoctrinated.

With your help, I hope to establish a system similiar to that existing in the rest of the Executive Branch.

I would appreciate your reviewing the attached draft. We can then meet to discuss it or, if you prefer, provide me with your ideas so that we can develop a proposal which will meet Paul's objectives.



Section II, Security Clearances

9. General

a. Only United States citizens shall be granted a personnel security clearance and indoctrinated for access to Sensitive Compartmented Information (SCI). All candidates for duty with the NSC, be they military or civilian permanent staff, detailees, consultants or contractors, must have a TOP SECRET (TS) security clearance and meet the eligibility requirements for access to SCI.

b. A candidate who has been selected for a position with the NSC and does not have an existing TS security clearance or recent Background Investigation (BI) will be subject to an investigation. The length of time it takes to complete any required investigation cannot be predetermined. Although existing collateral security clearances are generally transferable between agencies of the Executive Branch; SCI authorizations are not. Selectees without a prior security clearance or qualifying recent background investigation require a full BI update.

c. Selectees shall not be employed in a Sensitive Compartmented Information Facility (SCIF) until they have been indoctrinated for SCI. The reason for this prohibition is that SCIFs in the NSC contain secure voice communication systems in addition to SCI material in their ADP systems, in security cabinets and, in most cases, in daily use within the work areas. Due to the complexity of security measures to preclude unauthorized access, only SCI indoctrinated personnel shall be assigned to work in a SCIF.

d. The D/NSCSP shall provide the Director for Administration with a written notification of the security clearance and SCI authorization status of the selectee. The notification shall stipulate any prohibition against entry-on-duty pending completion of security clearance determinations and SCI authorizations associated with duty in the NSC. Should the selecting NSC Senior Director determine that the procedures outlined in paragraph 10, below, will cause an undue delay and that it is in the national interest to permit the selectee to enter-on-duty pending completion of the requisite BI or SCI eligibility determination, the NSC

Senior Director may take the action required in paragraph 11 a. or b., below, as appropriate.

10. Application for a TOP SECRET Security Clearance and Access to Sensitive Compartmented Information (SCI)

a. TOP SECRET Security Clearance. A promising candidate for a position in the NSC must complete an Standard Form 86 (Security Investigation Data for Sensitive Position) (SF 86) before being interviewed by the D/NSCSP. The interview addresses questions asked on the SF 86 and is designed to elicit information which will assist management in the selection process. The Executive Director, NSC will be advised by the D/NSCSP of any issues arising from the interview which could possibly result in denial of a TOP SECRET clearance or SCI indoctrination. If required, additional security forms will be furnished to the selectee by the D/NSCSP.

b. SCI Processing. Access to SCI is granted by the following consecutive steps:

(1). a determination by the NSC Senior Director that the position to be occupied by the selectee requires access to SCI ("need-to-know" determination);

(2). the selectee must have been the subject of a completed BI covering the most recent fifteen years of his or her life. A BI which meets these requirements, and is not more than five years old, will generally satisfy requirements for SCI indoctrination;

(3). a TOP SECRET security clearance must have been issued, or certified to, by the D/NSCSP;

(4). approval must be received from the CIA for SCI indoctrination; and

(5). indoctrination must be completed before access to SCI is authorized.

c. On receipt of notification from the CIA that the selectee has been indoctrinated for SCI, the D/NSCSP will send a written notification to the NSC Senior Director in whose office the selectee is assigned.

11. Exceptions to Investigative Requirements.

In exceptional cases, where a selectee has a BI more than five years old and has been continuously employed in the Executive Branch since his or her most recent qualifying BI, an NSC Senior Director may determine it is necessary or advisable in the national interest to request the D/NSCSP to grant the selectee an Interim TOP SECRET (ITS) security clearance or, if the selectee has a TS clearance but requires a current BI to

qualify for SCI indoctrination, to request access to SCI due to a "Compelling Need". An ITS clearance is not valid for access to SCI. The NSC Senior Director may take one of the following actions:

a. Request for Interim TOP SECRET. A

Senior Director may opt to request the selectee be granted an ITS clearance pending completion of the required investigation. The NSC Senior Director shall submit a written request to the D/NSCSP justifying the need for the ITS. Consideration will be given such request provided the selectee has been the subject of a current favorable National Agency Check and a new BI has been initiated. Because the granting of an ITS clearance does not qualify a selectee for eligibility for access to SCI, this option does not apply to a selectee who is to be assigned to an area accredited by the United States Secret Service as a Sensitive Compartmented Facility (SCIF) in which SCI material is openly stored (see paragraph 2. ae). Prior to permitting a selectee to enter-on-duty with an ITS clearance, the NSC Senior Director shall develop a security plan designed to ensure that the selectee is denied access to SCI in a closed storage SCIF (see paragraph 2. i). The security plan shall address the following actions:

(1). procedures to deny the selectee access to the cipher system code for controlling entry to the SCIF;

(2). procedures to deny the selectee access and lock combinations to security cabinets containing SCI;

(3). procedures to deny the selectee access and passwords to computers which contain SCI material;

(4). procedures to deny the selectee access to secure voice communications;

(5). procedures to ensure that, while in the SCIF, the selectee is under continuous escort by an SCI indoctrinated co-worker, and

(6). procedures for ensuring that the selectee will not receive SCI material via the mail distribution system or messenger system.

b. "Compelling Need" Request for Access to SCI

Selectees who have a final TS certified to by the D/NSCSP but require an updated BI for SCI indoctrination eligibility, may be eligible for early SCI indoctrination based on a justified "compelling need" established by the selecting NSC Senior Director. Under this option, once the NSC Senior Director has made his or her determination of the necessity for early access to SCI, he or she may submit a memorandum to the D/NSCSP, subject: "Compelling Need Request for Access to

SCI by (name of employee)". The request shall include the selectee's:

- (1). full name;
- (2). date and place of birth;
- (3). Social Security Account Number, rank/grade, and, if active duty military, branch of service;
- (4). duty title and SCI accesses required;
- (5). justification establishing the immediate need for access to SCI and an explanation as to why another indoctrinated passholder cannot perform the SCI related task until the passholder is granted SCI access through the normal process.

c. On receipt of the information required in d., above, the D/NSCSP will enclose the request with a formal request to the CIA. The latter request will include a copy of the passholder's most recent SF 86.

d. Passholder's with SCI access are subject to a periodic reinvestigation every five years.

11. Consultants

Consultants are subject to the same investigative requirements as passholders if they require access to TOP SECRET or SCI information. Once a prospective consultant has been tentatively approved for appointment, the D/NSCSP should be notified in order that expeditious action may be taken to identify and confirm existing clearances or to initiate any investigations considered appropriate for the level of access required.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

March 22, 1988

MEMORANDUM FOR JAMES T. MCCUE
MARY A. DIX
GEORGE VAN ERON

FROM: PAUL SCHOTT STEVENS *PS*
SUBJECT: Security Approval Required for
Entry-on Duty

As you know, the process followed in the selection of new staff for the NSC is designed to obtain the best qualified candidates for the job. Not the least important consideration is the question of security. The NSC is, if not the primary, certainly a major target of hostile intelligence services. As a result, the NSC must take all reasonable precautions to ensure that classified information, including codeword, can be accessed only by those persons with a proper level of security clearance and an established "need-to-know." In the NSC a Top Secret clearance with codeword authorization is mandatory. Unfortunately, from a security viewpoint, it is not unusual to have several individuals on duty in the NSC who are still in the clearance process for access to Top Secret and codeword information. This situation exists because of the shortage of candidates with the required clearances. Therefore, certain security measures must be taken to prevent unauthorized access to classified and codeword information by personnel who are in the clearance process.

Effective this date, candidates for NSC positions, be they military or civilian permanent staff, detailees or consultants, who do not have current SCI clearances, will not be authorized by me to enter-on-duty with the NSC absent concurrence by the Director, NSC Security Programs provided in writing to the Director of Administration. In most instances such concurrence will require the employing directorate to adopt appropriate procedures designed to preclude access to computer terminals, secure voice communications systems, and security cabinets containing classified and codeword information to which the new employee is not yet cleared for access. Such procedures should also address handling of classified mail, document and office access controls, and other security measures applicable to the particular office involved. I ask that Jim McCue, in cooperation with George Van Eron and Mary Dix, draw up for my review a minimum set of such procedures that can be provided to Senior Directors in case of such new hires within their directorates. Implementation of such procedures will be the responsibility of the respective Senior Director and his or her designated Security Manager. Upon my approval of such procedures, Mr. McCue is requested to forward this memorandum together with such procedures to NSC Senior Directors for their information.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

March 18, 1988

MEMORANDUM FOR: GEORGE VAN ERON

FROM: JAMES T. McCUE *gm*

SUBJECT: Security Requirements for TOP SECRET and
Sensitive Compartmented Information
(SCI)

As you know, I am in the process of developing an NSC Security Regulation (NSC/SR). One of the areas I am looking at pertains to the procedures for receiving, dispatching, and maintaining accountability registers of TOP SECRET and SCI documents. I realize the NSC has a system of accountability and control for documents received at the NSC. I'm not sure that subject documents, handcarried into NSC offices, are placed into an accountability system. The question is: with instructional requirements imposed by the NSC/SR, can the system in place be used as is, or with minor modification, so that the "Purpose" of the NSC security program, as outlined below, can be accomplished?

I would appreciate your reviewing the following objectives and discussing with me the feasibility of this approach.

A. Purpose

1. To provide, within each NSC office, a central control system for TOP SECRET and CODEWORD documents.

2. To establish an inventory system for the identity, location, and disposition of TOP SECRET and CODEWORD material.

3. To enable the NSC to take timely downgrading/declassification of documents no longer requiring high level classification.

4. To assist in identification of TOP SECRET and CODEWORD documents which may be destroyed or retired.

B. Requirements

1. Each NSC Senior Director's office will have one terminal dedicated for data entry to ACTIVE DOCUMENTS.

2. One primary and one alternate, using the same password, will be authorized to access ACTIVE DOCUMENTS. One will be designated the TOP SECRET CONTROL OFFICER (TSCO); the other will be the ALTERNATE TSCO.

3. NSC offices will be able to access only their database.

4. Only the TSCO/ALTERNATE will be able to access their own DESTRUCTION RECORD and the TRANSFER OF DOCUMENTS RECORD.

5. The Director NSC Security Programs will have override capability for access to each database.

6. The ACTIVE DOCUMENTS database will be a permanent record system.

7. Documents in the DESTRUCTION RECORD and TRANSFER OF DOCUMENT database will remain in the system for one year after which they will be automatically dropped. Hard copy Destruction Certificates and Transfer Receipts will be retained for three years.

8. Quarterly printouts will be required for each NSC office so that they can conduct an inventory. Requirements will be established in an NSC Security Regulation to be published.

9. For purpose of audit trails, the system should include a query capability to trail a specific document, via its control number, from one database to another, without running a query of the entire database.

C. Database

CONTROL RECORD
FOR TOP SECRET DOCUMENTS
AND
COMPARTMENTED DOCUMENTS

ACTIVE DOCUMENTS

NSC Document Control Number _____
Originator's Document Control Number _____
Title of Document _____
Date of Document _____

Document is Number _____ of _____ copies
Number of Copies Received _____
Date Received in NSC Office _____
Agency That Issued the Document _____
Date Document to be Downgraded _____
Date Document to be Declassified _____
Classification of Title _____
Codeword(s) _____
NSC Action Officer _____
Document Stored in Security Container # _____
Disposition of Document: (Check One)
____ Transferred to Another NSC Office on _____
____ Transferred Outside the NSC on _____
Identity of Receiving Activity: _____

Receipt Number _____
Transferred to Destruction Record _____
Downgraded _____ Declassified _____

DESTRUCTION RECORD

NSC Control Number _____
Title of Document _____
Document Copy Number _____
Classification at Date of Destruction _____
NSC Official Authorizing Destruction:
Name _____
Title _____
Office _____
Method of Destruction _____
Destroyed By:
Destroying Official _____
Witnessing Official _____
Destruction Record Number _____
Destruction Record location _____

TRANSFER OF DOCUMENT

NSC Control Number _____
Title of Document _____
Document Copy Number _____
Classification of Document at Time of Transfer _____
Transferred to _____
NSC Official Authorizing Transfer _____
Name _____
Title _____
Office _____
Date of Transfer _____

Document Receipt Number _____
Documented Receipted For On _____
Document Receipt Locatation _____

January 19, 1988

MEMORANDUM FOR THE NSC STAFF

FROM: PAUL SCHOTT STEVENS *PS*
SUBJECT: Mishandling of Classified Material

Our security office has brought to my attention its concerns that members of the NSC staff may be transporting or retaining classified material for work in their homes. This practice is strictly prohibited, as you all should know.

The key to the success of any information security program is the level of commitment to security requirements demonstrated by the personnel trusted to handle classified material. Let me make it clear that any unilateral, personal decision to remove classified material from appropriate custodial safeguards will be regarded as a very serious breach of that trust and dealt with accordingly. Anyone who has taken or is thinking about taking classified material out of the proper channels is urged to reconsider.

The intent to "get a few things done at home" may be well meaning, and understandable in view of the press of business here, but the risks occasioned to the national security (not to mention one's career) are simply too great. Considering the losses of classified material in recent years, there is every reason for members of the NSC staff to be especially conscious of such security requirements.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

January 14, 1988

ACTION**SIGNED**

MEMORANDUM FOR PAUL SCHOTT STEVENS

THRU: BRENDA S. REGER *BR*FROM: DORRANCE P. HOWLAND *DPH*

SUBJECT: Mishandling of Classified Material

The memorandum at Tab I is from you to the NSC staff warning them of the danger of working on classified material in their homes. As previously discussed with you, the NSC Security Office has received numerous indications, including an anonymous letter and one individual has been identified by name; that classified material is being worked on in NSC staffers' homes. The Security Office has issued a couple of security awareness bulletins via PROFS addressing the problem, but to no avail.

RECOMMENDATION

1. That you sign the attached memorandum for distribution within the NSC. *(as revised)*

Agree *DM* Disagree _____

2. That you speak to the senior directors at an ODSM or Wednesday staff meeting, to emphasize your concern in this matter.

Agree *DM* Disagree _____

Attachment

Tab I Stevens Memo to NSC Staff

NATIONAL SECURITY COUNCIL

WASHINGTON, D.C. 20506

MEMORANDUM FOR JAMES T. MCCUE
MARY A. DIX
GEORGE VAN ERON
CAROL PAQUETTE

7 April, 1988

FROM: PAUL SCHOTT STEVENS 
SUBJECT: Security Approval Required for
Entry-on Duty

As you know, the process followed in the selection of new staff for the NSC is designed to obtain the best qualified candidates for the job. Not the least important consideration is the question of security. The NSC is, if not the primary, certainly a major target of hostile intelligence services. As a result, the NSC must take all reasonable precautions to ensure that classified information, including codeword, can be accessed only by those persons with a proper level of security clearance and an established "need-to-know." In the NSC a Top Secret clearance with codeword authorization is mandatory. Unfortunately, from a security viewpoint, it is not unusual to have several individuals on duty in the NSC who are still in the clearance process for access to Top Secret and codeword information. This situation exists because of the shortage of candidates with the required clearances. Therefore, certain security measures must be taken to prevent unauthorized access to classified and codeword information by personnel who are in the clearance process.

Effective this date, candidates for NSC positions, be they military or civilian permanent staff, detailees or consultants, who do not have current SCI clearances, will not be authorized by me to enter-on-duty with the NSC absent concurrence by the Director, NSC Security Programs provided in writing to the Director of Administration. In most instances such concurrence will require the employing directorate to adopt appropriate procedures designed to preclude access to computer terminals, secure voice communications systems, and security cabinets containing classified and codeword information to which the new employee is not yet cleared for access. Such procedures should also address handling of classified mail, document and office access controls, and other security measures applicable to the particular office involved. I ask that Jim McCue, in cooperation with George Van Eron, Mary Dix and Carol Paquette, draw up for my review a minimum set of such procedures that can be provided to Senior Directors in case of such new hires within their directorates. Implementation of such procedures will be the responsibility of the respective Senior Director and his or her designated Security Manager. Upon my approval of such procedures, Mr. McCue is requested to forward this memorandum together with such procedures to NSC Senior Directors for their information.

cc: Donley

April 7, 1988

ACTION

MEMORANDUM FOR PAUL SCHOTT STEVENS

FROM: JAMES T. MCCUE *JTM*
SUBJECT: Security Approval Required for
Entry-on-Duty

At Tab 2 is a copy of your March 22, 1988 memorandum, establishing a policy for entry-on-duty with the NSC. Additionally, you asked me, in cooperation with George Van Eron and Mary Dix, to draw up for your review a minimum set of security procedures for new hires who do not meet full security clearance/access requirements.

One of the things that came out of our first meeting is that the White House Situation Support Staff (WHSSS) operates, personnel wise, independent of Mary's office.

In order to close the loop on security procedures, it appears that the WHSSS (Carol Paquette) should be formally included in your memorandum of March 22, 1988. At Tab 3 is a copy of a proposed modification of the memorandum, with Carol Paquette's name added to the addressees.

M. Dix 4-7-88
Mary Dix concurs.

RECOMMENDATION

That you sign the memorandum at Tab 1 with the original effective date of March 22, 1988. This will ensure that WHSSS is also aware of the new policy and the need to develop a minimum set of security procedures applicable to new hires in all NSC directorates.

Approve *JTM* Disapprove _____

Attachments

- Tab 1 - Proposed Memorandum
- Tab 2 - Original Memorandum
- Tab 3 - Highlighted Memo, Showing Changes

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

March 7, 1988

MEMORANDUM FOR NSC SENIOR DIRECTORS

FROM: PAUL SCHOTT STEVENS 
SUBJECT: Designation of Security Managers
and Alternates

In our continuing effort to enhance security within the NSC, it has been recognized that the success of any security program depends upon the full participation of all passholders. It is with this in mind that each NSC Senior Director is being called upon to increase his or her share of responsibility for an effective security program.

In order to assist Jim McCue, the NSC's newly-appointed Director of Security Programs, in carrying out his responsibilities, I request that each of you designate a point of contact within your office who will serve as liaison with Jim. Your designee will also serve as your Security Manager (SM). An Alternate Security Manager (ASM) should also be identified. You are requested to notify Jim, in writing, of the identity of your designated SM and ASM, along with their room and telephone numbers, within five work days of the date of this memorandum.

Once all SM's and ASM's have been identified, they will serve as Jim's points of contact on all security matters relating to your office. Likewise, all security matters involving your office, which require the assistance of Jim's office, will be processed via your designated representatives.

We expect this arrangement will best serve the interest of everyone and contribute significantly to improving security at the NSC.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

1157

February 12, 1988

MEMORANDUM FOR BRENDA S. REGER
JOHN F. LEWIS
GEORGE VAN ERON ✓
MARY A. DIX
RANDY MARONEY
CAROL PAQUETTE
NICK ROSTOW

FROM: DORRANCE P. HOWLAND *DPH*

SUBJECT: NSC Security Manual

The first edition of the NSC security manual is attached for your review and comment. An opinion is also requested as to whether the manual should be distributed by itself or included as an annex to the new staff manual. Please direct your comments to Brenda S. Reger or Dorrance Howland.

*70% finished
as of 7/6 per McCue -*

*will get to when Arlene
comes back.*

NATIONAL SECURITY COUNCIL

SECURITY MANUAL

REFERENCES

Director of Central Intelligence briefing for: National Security Council Document Handling Procedures and Responsibilities

Defense Investigative Service/Defense Security Institute, Security Awareness Bulletin, June, 1986, Computer Security

Defense Nuclear Agency, Security Manager's Handbook

Director of Central Intelligence Directive No. 1/21, Manual for Physical Security Standards for Sensitive Compartmented Information Facilities

Director of Central Intelligence Directive No. 1/14, Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information

Executive Order 12333, United States Intelligence Activities

Executive Order 12356, National Security Information

Information Security Oversight Office, Directive No. 1

Information Security Oversight Office, Marking

United States Department of State, Foreign Affairs Manual, Chapter 900, Security Regulations

United States Department of Energy, Security Education Handbook

United States Secret Service memorandum, Office Security

National Computer Security Center, Office of Standards and Product Evaluation, A Terminal User's Guide to Good Security Practices

National Security Agency, Chapter 803, Physical Security

National Security Agency, Security Guidelines

National Security Council, memorandum summarizing Executive Order 12356

White House Fact Sheet, National Operations Security Program

INDEX

PAGE

SECTION 1	GENERAL PROVISIONS.....	1
1-1	Purpose.....	1
1-2	Policy.....	1
1-3	Need to Know	1
1-4	Security in Depth Concept	1
1-5	Classification Responsibility	2
1-6	Use of Secure and Non-Secure Telephones	2
1-7	Operational Security	3
SECTION 2	PHYSICAL PROTECTION OF CLASSIFIED MATERIAL	4
2-1	Purpose	4
2-2	Protection of Classified Material	4
2-3	Area Control	4
2-4	Securing Area	4
2-5	After-hours Response	5
2-6	Accessing Area	5
2-7	Access List	5
2-8	General Precautions	5
2-9	Reporting Loss or Disclosure of Classified Material	5
2-10	Consultants	5
2-11	Changing Combinations	6
2-12	Room 208 Control	6
SECTION 3	TRANSPORTATION/REMOVAL OF CLASSIFIED MATERIAL FROM OFFICIAL PREMISES	9
3-1	Removal of Classified	9
3-2	Overnight Removal of Classified Material	9
3-3	Certification Upon Departure	9
3-4	Handcarrying Classified Material	9
3-5	Mail Transmittal	10
3-6	Courier Authorization	10
3-7	Courier Procedures	10
SECTION 4	SAFEGUARDING CLASSIFIED INFORMATION ...	12
4-1	General Procedures	12
4-2	Precautions	12
4-3	After Working Hours and During Lunch Periods.....	12
4-4	Security Clearance	13
4-5	Clearance Certification	14

SECTION 5	MARKING AND CLASSIFICATION OF DOCUMENTS.....	15
5-1	Classification of Information.....	15
5-2	Classifiers and Types of Classifications	15
5-3	Original classification.	15
5-4	Levels of Classification	16
5-5	Duration of Classification	16
5-6	Marking Requirements	16
5-7	Derivative Classification	17
5-8	Prohibitions and For Official Use Only	17
5-9	Declassification Authority	18
5-10	Control Markings	18
5-11	Cover Sheets and Storage	18
5-12	Marking on Special Categories	19
5-13	Documents Produced by ADP Equipment	20
5-14	Explanation of SCI	21
5-15	Accountability	21
5-16	Limited Access Programs	21
5-17	Preparation of SCI Documents	21
SECTION 6	TELEPHONE BOMB THREATS	22
	General	22
SECTION 7	PERSONAL COMPUTER SECURITY	24
7-1	General	24
7-2	Care of floppy disks	25
SECTION 8	USSS TECHNICAL SECURITY AND ESCORT PROGRAM..	26
8-1	Authority	26
8-2	Scope	26
8-3	Procedure	26
8-4	Schedule	27
8-5	Compliance	27
SECTION 9	PERSONNEL SECURITY	29
9-1	General	29
9-2	Anonymity	29
9-3	The NSC and Public News Media.....	30
9-4	Association with Foreign Nationals	30
9-5	Embassy Visits	31
9-6	Correspondence with Foreign Nationals	31
9-7	Unofficial Foreign Travel	31
9-8	Defensive Security Briefing	32
9-9	Membership in Organizations	35
9-10	Changes in Marital Status and Name Changes	35
9-11	Use of Illegal Drugs and Narcotics	36
9-12	Leak Investigations	36
9-13	Passes	36

SECTION 1

GENERAL PROVISIONS

1-1. Purpose - The purpose of this manual is to establish the policies and procedures for the protection of classified material entrusted to and generated by the the National Security Council (NSC).

1-2. Policy -

a. The NSC will use such physical deterrents, devices, controls and procedures as are necessary to limit access, knowledge or possession of classified material only to those persons who have been granted a security approval for the level or category of classified information involved and whose official duties require such access in the interest of promoting the national defense and foreign policy.

b. Each person having knowledge of, possession, or control of classified information is responsible for safeguarding that information in accordance with the provisions of this Manual.

c. The possession or use of classified information is restricted to approved locations or condition where security barriers and protective measures have been established to prevent unauthorized persons from gaining access.

1-3. Need to Know - Classified information is disseminated only on a strict "need-to-know" basis. The "need-to-know" policy means that classified information will be disseminated only to those individuals who, in addition to possessing a proper clearance, have a requirement to know this information in order to perform their official duties. No person is entitled to classified information solely by virtue of office position, rank or security clearance.

1-4. Security-in-Depth Concept - The protection of classified government information requires extraordinary precautions. To facilitate enforcement of the basic principle of the need to know is a system of internal barriers providing security in depth for compartmentation of physical space and access controls have been established around the Old Executive Office Building (EOB) generally and the NSC areas specifically. The concept of security in depth envisions a series of independent, but mutually supporting, barriers to provide safeguards for preventing access by unauthorized persons and the loss of control of classified materials. The success of this system depends upon the faithful exercise of responsibility by each individual having authorized access to classified information, including active participation in maintaining the integrity of established physical security procedures and practices.

All NSC personnel have the responsibility to assert the "need-to-know" policy as part of their responsibility to protect sensitive information. Determination of "need-to-know" is a supervisory responsibility. This means that if there is any doubt in your mind as to an individual's "need-to-know," you should always check with your supervisor before releasing any classified material under your control.

1-5. Classification Responsibility - Originators of correspondence, communications or documents with the NSC are responsible for ensuring that the proper classification, downgrading information and, when appropriate, proper caveat notations are assigned to such material. The Senior Director for Information Policy and Security Review is the declassification authority within the NSC and will also provide guidance in determining proper classification.

1-6. Use of Secure and Non-Secure Telephones - Two separate telephone systems for use in the conduct of official business are available within NSC spaces; the secure and the commercial, non-secure system. All NSC personnel must ensure that use of either telephone system does not jeopardize the security of classified information.

a. The secure telephone is beige in color and is provided and maintained by the White House Communications Agency (WHCA). The WHCA system provides the ability to discuss sensitive and up to Top Secret Codeword information. Personnel receiving calls on the secure phone may assume that the caller is authorized to use the system. However, you must ensure that the caller has a need-to-know for the information to be discussed. Additionally, the WHCA operator may extend calls to other national secure voice systems of the Department of Defense, State Department, and other Departments or agencies.

b. The outside, commercial telephone system, often referred to as the "black" telephone, is authorized for unclassified official business calls. The discussion of classified information is not permitted on this system. The non-secure telephone instrument should be placed one meter (39 inches) away from the other classified systems in the areas, including computer systems and the secure telephone.

c. In order to guard against the inadvertent transmission of classified information over the "black" telephone, an individual using the black phone in an area where classified activities are being conducted must caution other personnel in the area that the telephone is in use. Likewise, you should avoid if at all possible, use of the black phone in the vicinity of a beige, secure phone which is also in use. Attempts to use doubletalk to circumvent the restriction against the discussion of classified information over the non-secure telephone is prohibited.

1-7. National Operations Security Program - The President has signed a National Security Directive (NSDD) to establish a National Operations Security Program. The concept of operations security has been in existence for twenty years. With the priority of OPSEC now raised to the national level, it is important that all personnel become familiar with the concept.

a. OPSEC Process - The operations security process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified activity could be acquired in light of the the known collection capabilities of potential adversaries. Such evidence usually derives from openly available data. Certain indicators may be pieced together or interpreted to discern critical information. Indicators most often stem from the routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. Once identified, they are analyzed against the threat to determine the extent to which they may reveal critical information. Commanders and managers then use these threat and vulnerability analyses in risk assessments to assist in the selection and adoption of countermeasures.

b. OPSEC - Application of the concept is a systematic and proved process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

c. Threat and Vulnerability - In the OPSEC process, it is important to distinguish between analysis of threat and vulnerability, on the one hand, and implementation, on the other. Recommendation on the use of OP SEC measures are based on joint operational-intelligence analyses, but ultimate decisions on implementation are made by commanders, supervisors, or program managers who determine the aspects of a program or activity to be protected. The decision-maker with ultimate responsibility for mission accomplishment and resource management must have complete authority for determining where and how OPSEC will be applied.

SECTION 2

PHYSICAL PROTECTION OF CLASSIFIED MATERIAL

2-1. The purpose of this Section is to establish and prescribe the NSC staff's responsibilities and the physical security control procedures for the secure areas in which the classified work, storage and processing of classified material takes place. These areas are designated as Secure Compartmented Information Facilities (SCIF)s. Certification of the areas is the responsibility of the United States Secret Service (USSS).

2-2. Protection of Classified Material - The protection of classified material requires that the areas in which it is processed, discussed and stored must be under control at all times. During the normal work day, the properly cleared occupants of the area are responsible for maintaining that control. Whenever classified material is not under the personal control and observation of an authorized person, it will be stored in an approved locked container. Open storage of classified material, including classified waste in a burn bag, is not allowed unless specifically authorized in the certification letter by the USSS.

2-3. Area Control - The main entry door to a SCIF must be closed and under the control of the occupants at all times during the normal business day. This is facilitated by a keypad operated cipher lock that controls the entry door. The combination to the cipher lock should only be provided to those cleared personnel who have a need for unimpeded access to the area for the conduct of their official business. All others should be required to push the "V" for visitor button to gain access. Pressing the visitor button activates a bell or annunciator which warns the occupants that a visitor is coming into the area, and gives the occupants a chance to cover classified material or cease classified discussions. Uncleared visitors are provided an escort while in the secure space, and cleared visitors are provided only that material to which they are authorized.

2-4. Securing Area - At the close of business, the control reverts to alarms to detect unauthorized intrusion into the area, and the locks on the doors and windows to prevent surreptitious entry. When departing for the day after placing all classified material in storage containers, the inside locks on emergency exit doors should be checked to make sure they are in place, windows closed and locked, and the USSS control center called to notify them that the area is being secured. The alarm switch is placed in the secure mode and the occupants depart the area and lock the entry door from the outside, using either the keyed dead bolt or by spinning the dial on the built-in three position combination lock. After the locking procedure is accomplished, the door should be tried, to ensure the locking bolt is properly engaged.

2-5. After-hours Response - The USSS Uniformed Division is responsible for responding to alarms and for conducting routine patrol through the EOB after-hours. The Uniformed personnel are not cleared for SCI information, and therefore, a cleared NSC staffer must accompany the Uniformed officer to the area in which an alarm has sounded to provide escort. In almost all cases, this escort responsibility will be that of the Situation Room Watch Officer or his designee. Prompt response by the NSC in providing an escort is necessary under these conditions.

2-6. Accessing Area - When opening an area that has been secured, place the alarm control switch in the access mode and call the USSS Control Center at extension 4497, to announce your action.

2-7. Access List - Anyone accessing or securing a secure NSC space must be named on an access list that is on file with the USSS Control Center. To be placed on an access list requires SCI clearance. Senior Directors must authorize additions or deletions to an access list. The lists are maintained by the NSC Security Office.

2-8. General Precautions - The secure, controlled areas as described above are the only places where classified material should be stored, processed or discussed. Taking classified material home to catch up on some work is prohibited. When traveling, proper storage must be arranged during stopovers for rest periods. Your home, car pool, elevators, hallways, restaurants and other public places are not authorized areas for discussion of classified material; even if everyone involved in the discussion possess a proper clearance and a "need-to-know." The possibility that a conversation in a non-secure area could be overheard by unauthorized persons dictates the need to guard against classified discussions in non-secure areas. Additionally, classified information acquired during the course of your association with the NSC may not be mentioned directly, indirectly, or by suggestion in personal diaries, records, or memoirs.

2-9. Reporting Loss or Disclosure of Classified Information - The extraordinary sensitivity of the NSC product requires the prompt reporting of any known, suspected, or possible unauthorized disclosure of classified information or the discovery that classified information may be lost or not being afforded proper protection. Any information coming to your attention concerning the loss or unauthorized disclosure of classified information should be reported to your supervisor, the NSC Security Officer, the Situation Room Watch Officer or to the Administration Office, immediately.

2-10. Consultants - Authorized consultants and contractors engaged in work involving classified information may not store such material overnight on their office premises unless the Executive Secretary, with advice from the NSC Office of Security and the USSS, has granted approval for such storage. No classified information may be made available to consultants or contractors off the official NSC premises or transmitted to such persons except with the approval of the Executive Secretary and in conformity with proper security procedure.

2-11. Changing Combinations

a. Combinations to security containers and doors will be changed only by individuals having an appropriate security clearance and the authority to have access to the combination. The Security Office, Administrative Office and the USSS Technical Services Division (TSD) are authorized to change combinations under any of the following circumstances:

- (1) When the lock is initially put into use;
- (2) When an employee knowing the combination terminates employment or is permanently transferred to duties which no longer require employee's access;
- (3) Upon knowledge or suspicion that the combination has become known to an unauthorized person;
- (4) At least once every 12 months; and,
- (5) When equipment is taken out of service.

b. Combinations to safes must be placed on record with the Administration Office. The combinations are classified no lower than the highest category of classified material authorized for storage in the safe. Combinations for the three position locks built into the doors and the cipher locks must also be on file with the Situation Room, under the control of the Watch Officer. These combinations should be written on a 3 x 5 card, sealed in an envelope, dated and marked with the appropriate classification. It is the responsibility of each office to ensure the combinations are kept up-to-date. The USSS depends upon the combination records to be current in the Situation Room to facilitate emergency access to NSC areas, after-hours.

c. The combinations to safes and locks are to be memorized and not written on calendars or left in desk drawers or kept in one's wallet or purse.

2-12. As outlined above, all SCIF areas of the NSC are required to be under proper control at all times. The unique circumstances of the Cordell Hull Situation Support Facility (Room 208) is an area that requires extra attention. Those specific security guidelines are included below.

a. Security Requirements for Control of Cordell Hull Situation Support Facility (OEOB, ROOM 208)

- (1) The Cordell Hull Situation Support Facility (SSF) was created as a Sensitive Compartmented Information Facility (SCIF). The purpose of this facility is to

serve as an adjunct to the White House Situation Room for use in managing international and domestic crises impacting upon the national security. The classification of materials used in the management of national security situations is some of the most sensitive available within the U.S. Government. Therefore, only those individuals with Sensitive Compartmented Information (SCI) clearances are authorized unescorted access to the facility.

- (2) This facility was not designed for use as a conference facility for non-NSC functions.
- (3) Its construction was carefully monitored to ensure that every possible technological precaution was used to preclude unauthorized access to these most sensitive materials.
- (4) The following procedures have been established IAW Director of Central Intelligence Directives (DCIDs) 1/21, Minimum Standards for Physical Security for Sensitive Compartmented Information, 1/14, Personnel Security Requirements, 1/19, Requirements for Protection of Sensitive Compartmented Information, and Executive Order 12356, Minimum Requirements for Protection of Classified Material. They have been promulgated to ensure the security of Room 208 and the sensitive national security information which is contained therein.

b. Access Control Requirements:

- (1) Unescorted access to the area requires that the individual(s) have an SCI clearance.
- (2) Clearance must be verified through the NSC Security Office.
- (3) Ordinarily, the SSF will only be utilized by NSC personnel because the sensitive nature of the materials contained in this facility precludes use of the facility as a routine conference area.
- (4) In extraordinary circumstances, access to the facility by other than NSC personnel will be requested in writing to the Deputy Executive Secretary (Situation Support) of the NSC through the NSC Security Office. The request will include organization, senior individual to be at the session, classification of material to be used, point of contact, a list of attendees, and name of organization security officer. Each request will be reviewed and approved on a case-by-case basis. When approved, the event must be closely supervised by a properly cleared NSC staff member.

c. Equipment Control and Escort Program:

- (1) The equipment and furniture for Room 208 must remain in the control of the NSC as much as the space itself. Therefore, neither furniture, equipment or any item that is part of the Room 208 complex may be left unattended in hallways or other non-SCI areas. The threat of a possible implant of a listening device is too great and basic security procedure requires continuous control.
- (2) All non-NSC personnel accessing the area as visitors or maintenance must be closely escorted. Do not leave them alone.
- (3) The USSS will provide escort personnel for repairs and maintenance conducted in the briefing area of Room 208. They do this because of their technical security responsibilities there. To make arrangements, call the USSS duty desk at extension 4004 or 4005. This escort procedure does not extend to the audio visual support area for Room 208 or the reception area or its adjoining cloak room.
- (4) The United States Secret Service (USSS), Technical Security Division (TSD) provides periodic electronic sweeps of secure areas. To help maintain the integrity of the protected space, the USSS has developed a program which requires secure area occupants to report to the USSS when maintenance is performed on equipment or when new equipment, furniture or other articles are introduced into any area. The procedure is to fill out the check list (see Section 8) and send it to the TSD. That alerts TSD to a specific item that requires inspection and they will address that when conducting a periodic survey.

(d) Scheduling of the Facility:

- (1) Properly cleared NSC personnel may schedule use of the SSF through the White House Situation Support Staff, extension 7310.
- (2) Availability of the facility is subject to operational requirements of the WHSSS and the NSC.

SECTION 3

TRANSPORTATION/REMOVAL OF CLASSIFIED MATERIAL FROM OFFICIAL PREMISES

3-1. Classified material must not be removed from official premises except when necessary in the conduct of official meetings, conferences, or consultations and must be returned to safe storage facilities immediately upon the conclusion of the meeting, conference or consultation. Classified material must not be removed for reasons of personal convenience or be kept overnight in personal custody.

3-2. In unusual circumstances, requiring the overnight removal of classified material from official premises, prior approval from the Office of Security is mandatory. This is to insure adequate storage measures and compliance with the Executive Order 12356, implementing directives and other applicable regulations.

3-3. Certification upon Departure - When departing the NSC upon reassignment, resignation or retirement, each NSC employee or person detailed to the NSC, irrespective of rank, must certify as part of the exit procedure that:

- (1) classified NSC material is not being taken from authorized NSC control channels.
- (2) such material is not in their personal or household effects.

3-4. Handcarrying Classified Material - Persons handcarrying classified material will proceed as quickly and directly as possible from one secure area to another, and should not visit non-secure areas or conduct unofficial business enroute.

a. Classified material being handcarried within the White House Complex should be enclosed in an opaque container such as an envelope, briefcase, pouch, canvas bag, carton, etc. Classification or caveat markings will not be placed on the outside of the envelope or container but the name and/or organization of the transmitting office must be shown on the container or an attached tag or label.

b. In the Washington, D.C. metropolitan area, two appropriately-cleared and indoctrinated persons are required to handcarry Top Secret and SCI material when traveling by privately-owned, government or commercial automobile or other surface transportation. Unaccompanied appropriately-cleared personnel may routinely handcarry Top Secret or SCI material if traveling by authorized shuttle vehicle or chauffeured official vehicle. Properly cleared NSC Secretariat personnel, officially designated as couriers may handcarry Top Secret and SCI material unaccompanied in the Washington, D. C. area, using official government transportation. The material must be double wrapped.

The inner covering will be marked with the classification and any handling instructions, as well as the name and organization of the transmitting individual. An opaque covering such as an envelope, briefcase, pouch, canvas bag, carton, etc., will serve as an outer container. The outer container must be sealed or locked to prevent surreptitious access. The outer container will not be marked with classification, but will be marked, labeled or tagged with the instructions: "TO BE RETURNED UNOPENED TO THE NATIONAL SECURITY COUNCIL, OLD EXECUTIVE OFFICE BUILDING, 17TH AND PENNSYLVANIA AVENUE, WASHINGTON, D.C. 20506, Telephone 202-395-6313." Transmittal documents will be in accordance with Secretariat procedures if the material is to be left in the custody of an intended recipient; however, an inventory of the material being handcarried shall be retained in the transmitting organization.

3-5. Mail Transmittal - Confidential and Secret material may be sent via registered U.S. mail and U.S. military postal channels, provided that the material does not at any time pass out of U.S. citizen employee control and does not pass through a foreign postal system. Top Secret and SCI material must be transmitted via official diplomatic pouch, Armed Forces Courier Service (ARFCOS) or designated courier.

3-6. Courier Authorization - An NSC person designated as an official courier handcarrying classified material outside the Washington metropolitan area must have a letter signed by the NSC Security Officer authorizing the courier activity and the possession of the classified material. The Security Officer will also provide a courier briefing. Official NSC letterhead shall be used and the letter should contain the following:

a. The full name and identifying data that can be verified from separate identification carrying a photograph and descriptive data.

b. A description of the package containing the classified material.

3-7. Courier Procedures - When properly authorized, the courier should follow the procedures below:

a. Arrangements for overnight storage in appropriate government facilities must be made for the material at stops enroute to the destination, unless the material is retained in the personal possession and under the constant surveillance of the individual transmitting the material at all times. This does not mean the material may be kept in a hotel room while the traveler sleeps, but refers to overnight, "RED EYE" flights.

b. Classified material shall not be read, studied, displayed or used in any manner in public conveyances or places.

c. The classified information being carried shall contain no metal bindings and shall be contained in sealed envelopes, double wrapped. Should such envelopes be contained in a briefcase or

other carry-on luggage, the briefcase or luggage shall be routinely offered for opening for inspection for weapons. The screening officials may check the envelopes by X-ray machine, flexing, feel, weight, etc., without opening the envelopes themselves.

d. Opening or reading of the classified document by the screening official is not permitted.

SECTION 4

SAFEGUARDING CLASSIFIED INFORMATION

4-1. General Procedures.

- a. Employees using classified material or responsible for its custody must take every precaution to prevent deliberate or casual access to it by unauthorized persons.
- b. Classified material must not be left in unoccupied rooms or be left inadequately protected in an occupied office, or one occupied by other than security cleared employees.

4-2. Precautions.

- a. "Open/Locked" signs should be used on every safe or lockable cabinet containing classified material to indicate that the equipment is either open or locked.
- b. A security checksheet, SF 702, should be affixed to every security container in which classified material is stored. Employees opening or closing the container should complete the appropriate column. The national stock number of the SF 702 is 7540-01-213-7900.
- c. Personnel must insure that classified containers are locked prior to leaving the room unattended. When securing a combination lock, the dial must be turned at least four complete turns in one direction after closing. The employee should double check the lock to insure that it has been properly secured.
- d. Defects in or malfunctioning of storage equipment or locking devices must be reported immediately to the Office of Security or the Administrative Office. Uncleared contractors performing repair work on security containers must be closely escorted. Notification that work was performed on equipment in a SCIF area must be reported to the USSS under their escort program, as described in Section 8 of this manual.
- e. Before taking security containers, desks, or other furniture out of use that have been used to either store classified material or has been a work surface for classified material; that equipment must be inspected to ensure all classified material has been removed. Additionally, when taking a safe out of service, the standard combination of 25-50-25 should be set.

4-3. After Working Hours and During Lunch Periods

- a. Classified material must not be stored in desks or anywhere other than in lockable containers or safes.
- b. Classified material, including disposable material such as rough drafts, shorthand notes, extra and used carbon copies must

be safeguarded and locked in appropriate security containers whenever unattended. All typewriter ribbons and voice recording materials and burn bags containing classified trash must be safeguarded and locked in security containers at the close of business. Compliance with this requirement is a sound security practice and is advantageous to efficient administrative operations regardless of whether the media contain classified information. For these same reasons, a "Clean Desk" policy of securing all classified and unclassified documents is adopted.

c. In the instance where a keyed deadbolt is used to secure the area at the close of business, the USSS has determined that individual keys may be retained by the occupants during their tours with the NSC. The keys are accountable items. A lost key should be reported immediately to the Security Office, Administration Office or the USSS, Room 23, Old Executive Office Building (EOB).

4-4. Access - No person may be given access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties. Access to classified information shall be granted in accordance with the following:

a. Determination of Trustworthiness - No person shall be given access to classified information unless a favorable determination has been made as to the person's trustworthiness. The determination of eligibility, referred to as a security clearance, shall be based on such investigations as required in accordance with applicable standards. The NSC may issue an interim Top Secret clearance upon the receipt of a favorable FBI namecheck. Access to Sensitive Compartmented Information (SCI) is controlled by the minimum standards established and published by the Director of Central Intelligence.

b. Elected members of Congress and the Governors of the states are deemed to be trustworthy and eligible for a security clearance on a need-to-know basis, because of the trust placed in them through the election process. This privilege does not accrue to the staff members of these individuals. The staff members must be processed according to the minimum standards.

c. Determination of Need-to-know - A person is not entitled to receive classified information solely by virtue of official position or by virtue of having been granted a security clearance. A person must also have a need for access to the particular classified information sought in connection with the performance of official Government duties or contractual obligations. The determination of that need shall be made by officers having responsibility for the classified information.

4-5. Clearance Certification - The authorized discussion of classified material with appropriately cleared individuals from other agencies is a key factor in much of an NSC staffer's business. The Office of Security is the proper channel through which to pass and receive clearance information.

a. Incoming or outgoing certifications at the SCI level must go through the NSC Security Officer and be passed or received by the Office of Security within the Director of Central Intelligence, which in turn either receives or passes the SCI clearance to the intended receiver agency. A certain amount of this certification is conducted over the telephone, however, whenever possible, electric cables are preferred, and in some cases, required. Therefore, the earlier you submit your request for clearance, the more certain we can be of passing the information on time. Timeliness also provides an opportunity to fix any "glitch" that may occur.

b. The NSC Security Office may certify directly to, and receive from other agency security offices, the collateral clearances of Confidential, Secret and Top Secret. The certifications are passed via the telephone and through the mail at this level.

c. When making a classified visit to another agency, please provide the following:

- (1) Your full name
- (2) Your SSN
- (3) Agency to be visited
- (4) Date/s of visit
- (5) Person to be visited and telephone number
- (6) Specify clearance - TS/SI/TK/BYC/G

d. When planning to receive a visitor, please request that the visitor provide the NSC with their corresponding information, through their security office.

SECTION 5

MARKING AND CLASSIFICATION OF DOCUMENTS

5-1. Classification of Information - U.S. Government information is currently classified under the authority of E.O. 12356, signed by the President on April 2, 1982, and only for reasons of national security. The authorized classification levels are CONFIDENTIAL, SECRET and TOP SECRET, and relate to the severity of damage to the national security which would result from the unauthorized disclosure of the information. The E.O. also identifies the categories of information which can be considered for classification.

5-2. Classifiers and Types of Classification.

a. Original classification authority is granted by the President to the heads of executive departments and agencies requiring this authority. These classifiers are further authorized to delegate classification authority in writing to those officials with a government organization who require the authority to fulfill the terms of the Executive Order.

b. Information may also be derivatively classified either from source documents or authorized classification guides specifying the exact types of information which must be classified within each agency, between agencies or across the Intelligence Community.

5-3. Original classification - three tests must be met for you to originate a classified document:

a. You must be authorized in writing to classify documents originally. All the professional NSC staff members are authorized to classify at the "SECRET" level. Only the National Security Advisor and his Deputy are authorized to originally classify at the "TOP SECRET" level.

b. The information being classified must fall within one of the ten classification categories:

- (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 and 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 requires 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

c. Finally, the unauthorized disclosure of the information in one of these categories must reasonably be expected to cause damage to the national security.

* Foreign Government Information, Foreign sources or Intelligence Sources or Methods - 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 and, therefore, presumptively warrants classification at least the CONFIDENTIAL level.

5-4. Levels of Classification are to be assigned on the basis that unauthorized disclosure could be expected to cause the following levels of damage to the national security:

TOP SECRET	--	exceptionally grave damage
SECRET	--	serious damage
CONFIDENTIAL	--	damage

5-5. Duration of classification - The "review in six years" requirement of Executive Order 12065 has been dropped. Information shall now be classified for 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. When it is impossible to determine a specific date or event for declassification, the marking need only show that it must be reviewed prior to declassification. Use of the designation "Originating Agency's Determination Required" or "OADR" on the "DECLASSIFY ON" line will ensure that the information must be reviewed by the NSC before it can be declassified.

5-6. Marking Requirements - At a minimum, each page of the classified document must show the highest level of classified information contained therein, and the first page of each copy of all classified documents must indicate:

- a. The highest level of classification assigned within the document;
- b. The name of the original classifier (this may be either the drafter or the document or the approver);
- c. The agency of origin; and
- d. The date or specific event when the information can be declassified, or if unable to determine one, substitute "OADR."

- (1) The requirements for "a" and "b" may already be met if the document is on NSC or White House letterhead stationery and is signed by an original classifier.
- (2) Portion Marking - A partial waiver has been granted to the NSC Staff. Portion marking is not required for classified information in memorandums created by the NSC Staff or internal White House/Executive Office of the President use only. (It is recommended that you continue to portion mark your Weekly Reports and titles or subject lines on all such internal memorandums). However, documents being sent to other agencies must be portion marked to indicate clearly portions that are classified and at what level, and those that are unclassified. Each paragraph and title must, therefore, be followed by its appropriate classification. Special care should be taken to ensure that documents created for the signature of the President, APNSA, and other White House officials are done correctly.

5-7. Derivative Classification - If you are cleared to a particular classification level, you may extract or summarize information from classified documents originated within the White House and the NSC or received from other agencies even if you do not have the original classification authority for that level. For example, if using information at the TOP SECRET level when you are only authorized to classify originally at the SECRET level, you must note on the document you are creating that it is derivatively classified and then carry forward the appropriate identification and markings from the original document or documents.

5-8. Prohibitions - the Executive Order prohibits the following:

- a. Use of such terms as "SENSITIVE," "FOR OFFICIAL USE ONLY," "LIMITED OFFICIAL USE," and "ADMINISTRATIVE" in conjunction with classification markings.

Note: Separate from classified information markings is the term "FOR OFFICIAL USE ONLY" (FOUO). This designation is used to identify that official information or material which, although

unclassified, is exempt from the requirement for public disclosure and which, for a significant reason, should not be given general circulation. Each holder of "FOR OFFICIAL USE ONLY" information or material is authorized to disclose such information or material to persons in other departments or agencies of the Executive and Judicial branches when it is determined that the information or material is required to carry out a government function. The recipient must be advised that the information or material is not to be disclosed to the general public. Material which bears the "FOR OFFICIAL USE ONLY" caveat does not come under the regulation governing the protection of classified information, and the unauthorized disclosure of information so marked does not constitute an unauthorized disclosure of classified defense information. The NSC telephone listing of staff members is an example of information that could be marked "FOUO." NSC policy prohibits the unauthorized disclosure of information designated "FOR OFFICIAL USE ONLY." Appropriate administrative action will be taken to fix responsibility and to apply corrective and/or disciplinary measures in cases of unauthorized disclosure of information which bears the "FOR OFFICIAL USE ONLY" caveat. Reasonable care must be exercised in limiting the dissemination of "FOR OFFICIAL USE ONLY" information.

b. 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.

5-9. The declassification authority is placed with the Senior Director for Information Policy and Security Review, Brenda Reger. All questions on declassification should be directed to her at extension 3103.

5-10. Control Markings - Not only must both the page and paragraph show classification level, but also control marking as prescribed by Director of Central Intelligence Directive 1/7. These include NOFORN, NOCONTRACT, PROPIN, ORCON, and WNINTEL, abbreviated for page markings and written as NF, NC, PR, OC, and WN for portion marking purposes. These controls are placed after the classification level when labeling the paragraph and must be stated prominently in one place, either top or bottom, on the page as well as on any cover sheet. To override any of the control markings, the originator must be consulted for approval.

5-11. Cover sheets and storage - All classified information should be identified by an appropriate cover sheet to protect against inadvertent disclosure and to serve as a reminder for compliance with storage and transmission requirements. Confidential and Secret documents may be stored in GSA approved safes with 3-way combination locks. Top Secret material and Sensitive Compartmented Information must be stored within approved, alarmed and secured vault-type areas with authorization to store such material.

5-12. Marking on Special Categories of Material - Security classification and declassification instructions assigned by the classifier shall be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal or similar device, on classified material other than paper copies of documents, and on containers of such material, if possible. If marking the material or container is not practicable, written notification of the security classification and declassification instructions shall be furnished to recipients. The following procedures for marking various kinds of material containing classified information are not inclusive and may be varied to accommodate the physical characteristics of the material containing the classified information and with organizational and operational requirements.

a. Charts, Maps, and Drawings - Charts, maps, and drawings shall bear the appropriate classification marking under the legend, title block, or scale, in a manner that differentiates between the overall classification of the document and the classification of the legend or title itself. The higher of these markings shall be inscribed at the top and bottom of each such document. When folding or rolling charts, maps or drawings would cover the markings, additional markings shall be applied that are clearly visible when the document is folded or rolled.

b. Photographs, Films, and Recordings:

- (1) Photographs - Negatives and positives shall be marked with classification markings and kept in containers bearing conspicuous classification markings. Roll negatives shall be marked at the beginning and end of each strip and single negatives marked with the classification. Each photographic print shall be marked with the classification at the top and bottom of the face side and, where practicable, the center of the reverse side. Caution must be exercised when using self-processing film or paper to photograph or reproduce classified material, since the negative of the last exposure may remain in the camera. All component parts of the last exposure shall be removed and destroyed as classified waste or the camera shall be protected as classified material.
- (2) Transparencies and Slides - Classification markings shall be shown on each transparency or slide. Other markings, when practical, shall be shown on the border, holder or frame.
- (3) Motion Picture Films - classified motion picture films shall be marked at the beginning and end of each reel by titles bearing the classification. Such markings shall be visible when projected on the screen. Reels shall be kept in containers bearing conspicuous classification markings.

- (4) Recordings - Recordings, sound or electronic, shall contain at the beginning and end a statement of the assigned classification which will provide adequate assurance that any listener or receiver will know that classified information of a specified level of classification is involved. Recordings shall be kept in containers or on reels that bear conspicuous classification markings.

c. Removable Automatic Data Processing and Word Processing Storage Media - Removable information storage media, employed with automatic data processing (ADP) systems and typewriters or word processing systems shall bear external markings and internal notations sufficient to assure that any recipient of the media, or of the classified information contained therein when reproduced by any means, will know that classified information of a specific classification level is involved. This category media and devices that store digitally recorded information are generally intended to be mounted or removed by the users or operators. Examples include magnetic tape reels, cartridges and cassettes, removable discs, disc cartridges, disc packs and diskettes, paper tape reels, and magnetic cards. Once a piece of removable magnetic storage media has been used for the processing of classified information, it will always be treated and protected as classified until sanitized by an approved method.

d. Nondemountable Data and Program Storage Media - All nondemountable data and program storage media, such as Winchester type disk units, used for the processing of classified data must be treated as classified unless declassified with approved methods or techniques. When removed from operational use such storage media will be marked with the appropriate external classification.

5-13. Documents Produced by ADP Equipment - at a minimum, the first page, and the front and back covers, if any, of documents produced by ADP equipment shall be marked with the overall classification. Classification markings of interior pages may be applied by the ADP equipment or by other means. When the application of declassification instructions and other markings by the ADP equipment is not consistent with economic and efficient use of such equipment, such instructions and markings may be applied to a document produced by ADP equipment by superimposing upon the first page of such document a "Notice of Declassification Instructions and Other Associated Markings." Such notice shall include the date for declassification or review for declassification and all other such applicable markings. If individual pages of a document produced by ADP equipment are removed or reproduced for distribution to other users, each such page or group of pages shall be marked by superimposing on each such page or group of pages, a copy of any "Notice of Declassification instructions and Other Associated Markings" applicable to such page or group of pages.

5-14. Explanation of SCI - Sensitive Compartmented Information (SCI) is often referred to as codeword information and differs from collateral Confidential, Secret and Top Secret firstly because it is contained in distinctly named channels and secondly because codewords within the the channel serve to identify and protect specific kinds of intelligence information. SCI is always intelligence information and each channel has been designed to protect a particular technology. All SCI must be prepared, handled and controlled according to Director of Central Intelligence Directive (DCID) 1/19 which describes: classification levels, channels, codewords, control markings, cover sheets, document numbers, copy numbers, courier receipts, document receipts and the provisions of a complete audit trail for hard copy documents.

5-15. Accountability - Each copy of an SCI document must have strict accountability with receipts and logs showing the document's location from origination to destruction. The NSC Secretariat maintains the accountability system for this material and should be contacted with specific questions.

5-16. Limited Access Programs - There are also other, limited access programs, often codeworded to protect the integrity of the program and limit access to only those involved in it. These may utilize information gained from SCI or by collateral means. These programs usually have distinctive cover sheets and may employ more specific handling controls than those for other classified information. It is required in these cases that you not only abide by the basic rules, but also those imposed by the special program. In no case should the handling procedures be less than those prescribed by the regulations, just because the program may be special or exclusive. Accountability for these program documents within the NSC is the Secretariat.

5-17. Preparation of SCI Documents.

a. SCI finished intelligence documents not only require the classification level at the top and bottom of the page as well as any control markings and the previously described portion-marking, but also channel indicators, appropriate codewords, document numbers, copy numbers, complete records of distribution by the originating office and distinctive cover sheets by color or format indicating the type of information contained therein.

b. The channel and document number must be indicated on every page of the document as well as the classification level top and bottom and any codeword or control markings. Nevertheless, keep in mind sufficient margins top and bottom are required in order to accommodate all of this information. The channel, classification level, control markings and any sub-compartments should be indicated on the cover sheet; the codewords should only appear on the inside pages. According to the Community regulations associated codewords are classified within the channel, thus indicating them on the cover sheet would result in classifying the cover sheet itself.

SECTION 6

TELEPHONE BOMB THREATS

General: The telephone provides a convenient method of expressing an anonymous threat. In the case of a telephone bomb threat, any NSC staff person is a potential recipient of such a call. The following are actions which should be taken in the event a telephone bomb threat is received.

a. Immediately indicate to a co-worker that a bomb threat call has been received. Request the co-worker to notify the USSS 24 hour duty desk at X4004 or the USSS Uniformed Division Control Center at X4497. The extension on which the threat is received should be identified. The USSS will record the call and initiate an investigation.

b. Keep the caller talking. Make notes on what is said by the caller, quoting the exact words of the caller, if possible. Attempt to determine the following information about the bomb in the order listed:

- (1) Where is the bomb?
- (2) What does it look like?
- (3) When is it going to explode?
- (4) What will make it explode?
- (5) How can it be deactivated?
- (6) Why was the bomb set?

c. An attempt should be made to determine the following information about the caller:

- (1) Identity.
- (2) Location.
- (3) Phone number where caller can be reached.
- (4) Age and sex.
- (5) Speech characteristics, i.e., accent, colloquialisms.
- (6) Manner of speech, i.e. rational, irrational, emotional, angry, deliberate, slurred, etc.
- (7) Background sounds, i.e., traffic, music, party/bar sounds, office machines, voices. etc.
- (8) Did the caller appear familiar with the building against which the bomb threat was made? Did the caller provide significant detail concerning the nature of the bomb?

d. As obvious as it may appear, nevertheless, advise the caller that detonation of the bomb could result in injury or death to innocent people. This may influence the caller to provide more information.

e. After the caller has terminated the conversation, immediately notify the USSS Duty Desk of all information obtained. All bomb threat notices should be treated as if an explosion will result. All bomb threats will be thoroughly investigated. Individuals making bomb threats, by whatever means, are subject to prosecution for violation of Section 844, Title 18, U.S. Code which provides for imprisonment for not more than five years or a fine of not more than \$5,000, or both.

f. There are no rules or differentiation between a hoax call and a real bomb threat. All bomb threat information received should be immediately reported to the USSS. No further action should be taken by the call recipient, with respect to the reported bomb, prior to notifying the USSS.

SECTION 7

PERSONAL COMPUTER SECURITY

7-1. As more and more Personal Computers (PC's) enter the workplace, the risk of loss, disclosure, or compromise of classified and/or sensitive information processed on them rises significantly. The power and utility of PC's attract a large number of users with a great variety of applications. Because of this attraction, as well as the accessibility of the systems and their inability to discriminate between the "good" user and the "bad", you should observe the following practices to ensure a safe and secure computing environment.

- a. Limit Access to Your PC - Know those who use it, service it, and repair it. Use system lock-down or power switch locking devices when available.
- b. Label All Diskettes - Indicate the classification level of the data or application on the diskette. Unclassified or sensitive diskettes should also be labeled.
- c. Avoid leaving classified and/or sensitive data in the PC.
- d. Remove diskettes and store them securely when not in use.
- e. Turn off the PC after using it. This will usually clear data from the memory, but check the manufacturer's documentation to be sure.
- f. Diskettes, or other magnetic storage media, that have been exposed to classified and/or sensitive data or applications assume the classification level of the data or application.
- g. Do not allow storage media on which classified and/or sensitive data or applications have resided to leave controlled channels until they have been degaussed (demagnetized). Check with the NSC security officer on proper disposal and maintenance sanitization for procedures.
- h. Do not trust copy commands, as most PC operating systems copy files by sectors. Classified and/or sensitive data from a previous file may be inadvertently transferred to another file or storage medium.
- i. Do not trust data deletion commands such as "remove," "erase," or "delete." The data may not be removed from the diskette although the file name may be deleted.
- j. PC's connected to other computers can be accessed and files, applications, and even the operating system can possibly be changed without your knowledge. Again, turn off the PC or disconnect if from other computers when not using it.
- k. Beware of borrowed or unsolicited software. These may contain programs or instructions specifically designed to capture or alter your data or application.

1. Make backup copies of all your data files and applications.

7-2. Care and keeping of your floppy disks and computer equipment are just as important as the security aspects of locking up the information for the long term protection of the information. The following tips will help.

a. Keep disks in their protective jackets when not in the drive unit.

b. Keep disks stored upright in their boxes.

c. Keep disks clear of eraser crumbs, dust, and smoke particles.

d. Use a felt tip pen when writing on the disk label pencil or ball point pressure can destroy floppy precision.

e. Make up copies. Then store them in a facility separate from the originals.

f. Don't touch the disk surface. It's easily contaminated, so something as minor as a fingerprint can cause error. On a dry day, your finger could have enough electrostatic charge to damage them permanently.

g. Don't use alcohol, thinners, or freon to clean the disk. Chemical fumes can endanger the magnetic coating, so don't expose it to solvents like nail polish or duplicating machine fluids.

h. Don't expose the disk to magnetic or magnetized objects. Data can be destroyed, scrambled, or wiped out completely. A color TV, CRT, electric motor, or other devices can destroy data integrity. Screwdrivers, paper clips, car keys, or any metal object may also be magnetized.

i. Don't put a telephone on top of a disk, the disk drive, or a box of disks. One ring can cause damage.

j. Don't expose disk to power supply units.

k. Don't bend, fold, or use rubber bands or paper clips in the disk. Any wrapping can lead to mistracking.

l. Don't rest heavy objects on the disk. It can cause a crimp that would lead to mistracking.

m. Protect your floppy at least as well as you would the data that's on it.

SECTION 8

USSS TECHNICAL SECURITY AND ESCORT PROGRAM

8-1. Authority - Under Executive Order 12333, the Technical Security Division (TSD) of the USSS is responsible for providing audio countermeasures inspections within the White House/OEOB Complex and other areas as designated by the Secretary of the Treasury or the President. In compliance with this Executive Order, the NSC spaces are periodically inspected to detect the presence of unauthorized listening/transmitting devices. The occupants of an area are reminded that their assistance is needed to maintain the security of the office.

8-2. Scope - During the inspection or "sweep", a fully cleared TSD team uses numerous techniques to detect the presence of unauthorized listening or recording devices, commonly known as "bugs". Upon completion of the sweep, it is imperative that adequate security be maintained on the areas to ensure the integrity of the sweep. A list of the TSD team members and their clearances is on file in the Situation Room.

8-3. Procedure - During working hours when the area is no longer under the security of intrusion alarms or Uniformed Division officers, it is incumbent upon the personnel in the area to keep the area secure. To support the program, the following procedures should be observed.

a. Escort all tradesmen, electricians, carpenters, telephone men, equipment repair personnel that enter the area to perform any work. The fact that work was accomplished in your area must be reported immediately to TSD. This should be done using the escort form furnished by TSD (see attached).

b. Any new furnishing brought into the area, or present furnishings removed and returned, should be reported on an escort form. Once a piece of furniture has been inspected and brought into a SCIF, it must remain under control. Do not allow the equipment to remain unattended in a hallway or other uncontrolled area as this nullifies any electronic sweep.

c. The cleaning personnel are not cleared and should also be escorted, however, their entry into the SCIF does not have to be reported to TSD.

d. The commercial telephone will be inspected during a sweep, however, no guarantee can be made against unauthorized interception of your conversation or a "tap", so never discuss classified information on a commercial telephone.

e. Report any suspicious activity or changes in your area for which you cannot account. Report such occurrences from a telephone outside your area to the TSD duty desk on 395-4005 or the TSD office on 395-6396.

8-4. Schedule - Most of the sweeps take place after normal working hours. However, if you are present during an inspection, please continue with your usual functions and make no mention of what is taking place in the office. If you have a question or wish to speak to a team member, motion for him/her to step outside the office to talk. Prior to the arrival of the inspection team, no discussion that a sweep will take place should be held within the area. It should be noted that if during an after-hours sweep, the TSD team comes across a safe that is not locked or classified material not properly stored, they are obligated to write up a security violation.

8-5. Compliance - It is important that the above procedures be followed. "Bug" devices currently available can be introduced into your area in less than one minute. It is the responsibility of each of us to assist in this aspect of "security in depth" to keep the office environment secure. The USSS appreciates the cooperation.

Technical Security Division
Technical Surveillance Countermeasures Section

DATE: _____

From: _____

Office: _____ Room # _____
(If applicable)

Name of workman _____

Company he/she works for _____

Area of room where work was accomplished.

The work accomplished was: (Check appropriate boxes)

Installation of new equipment/furnishings - - - - - ☐

Repair of existing equipment/furnishing - - - - - ☐

Repair of telephone equipment - - - - - ☐

Plastering, painting, etc. - - - - - ☐

Other, specify _____ ☐

The workman was escorted by _____

Serial number of equipment worked on _____

If you have any questions concerning the escorting or execution of this form please call 395 - 4005 or 395 - 6396 for assistance.

After completing this form please forward as soon as possible to TSD to Room 572, the appropriate follow-up action will be scheduled.

SECTION 9

PERSONNEL SECURITY

9-1. The most important aspect of any security program is the role played by you, the individual staff member, regardless of your rank or position. Your recognition of your responsibility to protect classified material will finally determine the success of the program. Many of the parts of the "security-in-depth" system, such as alarms, guards, locks, fences and technical sweeps are somewhat removed from the control of the individual staff member. There are, however, other aspects of the security program in which you play a more personal part. Some of those issues are discussed below.

9-2. Anonymity - Perhaps one of the first security practices with which a person new to the NSC should become acquainted with is the the practice of anonymity. In an open society such as ours, this practice is necessary because information which is generally available to the public is available also to hostile intelligence. Therefore, the NSC mission is best accomplished apart from public attention. Basically, anonymity means that NSC personnel are encouraged not to draw attention to themselves and their association with the NSC. Personnel are also cautioned neither to confirm nor deny any specific questions about NSC activities directed to them by outsiders who have no "need-to-know."

a. Certainly you may tell your family and friends that you are employed or assigned to the NSC. There is no valid reason to deny them this information. However, you may not disclose to them any information concerning specific aspects of classified work or special projects, unclassified but sensitive, on which you may be working. You should also request that they not publicize your association with the NSC.

b. Should strangers or casual acquaintances question you about your place of employment, an appropriate reply would be the Old Executive Office Building in Washington. As prestigious as it is, avoid saying to strangers or people you barely know, that you work at the White House.

c. When you inform someone that you work for the NSC, you may expect the next question will be, "What do you do?" It is a good idea to anticipate this question and to formulate an appropriate answer. Do not act mysteriously about your employment, as that would only succeed in drawing more attention to yourself. Say you are a staff assistant, secretary, staff member, analyst, or that you are an economist or study international affairs or some other general title that does not indicate specifically how your talents are being applied to the mission of the NSC.

9-3. The NSC and Public News Media - It is not unusual for the NSC to be the topic of reports in public news media. The White House Press Office represents the NSC in matters involving the press or other media. That organization serves as the NSC's official voice. In order to protect sensitive aspects of NSC activities, NSC personnel must refrain from either confirming or denying any information concerning the NSC or its activities which may appear in the public media. Also, to speak out publicly about a specific issue may constitute an unauthorized disclosure of classified information and violations of law.

9-4. Association with Foreign Nationals - To help protect sensitive information and material from deliberate or inadvertent disclosure, the NSC has adopted a policy concerning association with foreign nationals. The policy considers the well-being of NSC personnel who, by virtue of their access to sensitive classified information, are potential targets for hostile Intelligence efforts. Personnel are, therefore required to report to Security certain types of relationships with foreign nationals.

a. The first type of relationship which must be reported is any contact between NSC personnel and citizens or representatives of Communist-controlled countries, no matter how brief or apparently trivial the contacts may be. This reporting is further required by a National Security Decision Directive, Number 197. The requirement is based on the knowledge that citizens and representatives of these countries have, in the past, been frequently identified as being involved in intelligence gathering activities. Such activities have included the collection or personal information to aid in the targeting and subsequent recruitment of personnel associated with sensitive U.S. government organizations.

b. The second type of relationship which must be reported concerns itself with close and continuing contact with a foreign national. Any regular, frequent contact with a foreign national must be reported to Security. United States National Foreign Intelligence Board security policy requires that personnel avoid associations with foreign nationals which may be characterized by ties of kinship, affection or obligation.

c. Casual, inadvertent, or irregular contacts which arise from normal living and working in the community normally need not be reported. If, however, you feel that a contact is in any way suspicious, it should be reported immediately.

d. During the course of casual contacts with foreign nationals, NSC personnel are encouraged to extend normal social amenities. By no means should you act mysteriously or draw attention to yourself and possibly to the NSC by displaying an over-cautious attitude. Naturally, your affiliation with the NSC and the nature of your work should not be discussed.

e. Whenever any doubt exists as to whether a situation should be reported or made a matter of record, you should decide in favor of reporting it. In this way, the situation can be evaluated on its own merits, and you can be advised as to your future course of action.

9-5. Embassy Visits - Since a significant percentage of all espionage activity is known to be conducted through foreign embassies, NSC policy discourages visits to embassies, consulates or other official establishments of a foreign government. Each case, however, must be judged on the circumstances involved. Therefore, any individual who plans to visit a foreign embassy should consult with their immediate supervisor or the security office.

9-6. Correspondence with Foreign Nationals - NSC personnel are discouraged from initiating correspondence with individuals who are citizens of foreign countries, particular with citizens of those nations whose interests are inimical to the interests of the United States. Unofficial correspondence with citizens of Communist-controlled countries is prohibited. Casual social correspondence, including the "pen pal" variety, with foreign acquaintances who are not nationals of or in any way connected with, Communist or Communist-controlled countries is acceptable and need not be reported.

9-7. Unofficial Foreign Travel - In order to further protect information from possible compromise resulting from coercion, entrapment, exploitation, interrogation or capture of NSC personnel by hostile nations or groups, the NSC establishes certain policies and procedures concerning unofficial foreign travel.

a. All NSC personnel, civilian or military, who are planning unofficial foreign travel must submit a proposed itinerary to Security at least fifteen working days prior to their planned departure from the United States. These itineraries will be reviewed in light of the existing situation in the country or countries to be visited, and a recommendation whether the area should be visited. In cases where the hostile threat is so great, and these areas change with time and political climate of the world, the Executive Secretary may prohibit the unofficial foreign travel. The purpose of this policy is to limit the risk involved with travel to areas of the world where a threat may exist to personnel and to the knowledge of current classified NSC information and by derivation, the knowledge of classified material of many other intelligence agencies within the U.S. Government which NSC personnel may possess.

b. In this context, unofficial travel to Communist or Communist-controlled countries is prohibited without the review and concurrence of the NSC Executive Secretary.

c. Unofficial foreign travel to Canada or the border areas of Mexico need not be reported unless some unusual or special circumstance is associated with the travel, e.g., unusual or extended personal involvement with foreign nationals, difficulties with local police or governmental authorities.

9-8. Defensive Security Briefing - The following items are brought to your attention to furnish you with a security guide which can be utilized in conducting your official business in a manner affording the greatest personal safety and the most secure method for safeguarding classified information while traveling officially in Communist countries or other unfriendly foreign countries, or when attending any international conference or participating in scientific, cultural or commercial exchange programs where representatives of Communist or unfriendly countries are expected to be in attendance.

a. Any classified information required during the foreign travel should be transmitted in advance to the most convenient United States installation which might be visited. If for any reason prior transmission of information is impossible or impractical, the traveler must be designated as an official courier, complete with courier letter and briefing, as discussed in Section 3-6 of this manual.

b. Before departing the United States the traveler should ascertain the location of the U.S. Embassy, Consulate and/or military installation nearest your destination. Upon arrival, classified documents should be stored with the security officer of the U.S. Embassy, Consulate or military installation. Although it may have been necessary for an authorized courier to carry classified documents to a foreign country, for the purpose of meeting, it often is possible to have these documents returned to the U.S. via the U.S. Embassy pouch system.

c. Classified notes made at overseas meetings will be safeguarded at all times; they may not be retained in hotels or temporary residence overseas. Classified documents will be deposited for temporary storage with the Security Officer of the nearest U.S. Embassy, Consulate, or military installation, and that official should be requested to have the classified information returned via Diplomatic Pouch.

d. United States classified documents will not be passed to foreign government representatives at conferences. Classified document will be released only through established channels, government to government.

e. The carrying or keeping of overseas diaries is discouraged except as may be necessary for the purpose of transportation, expense accounts, travel vouchers, etc. Under no circumstances will such notes contain personal opinions, names of personalities or classified information.

f. Personal correspondence passing through the international mails is subject to control and censorship by various countries. In certain areas the censorship is apparent and exercised in accordance with law or custom. In other areas, while it may be legal, certain technical means may be employed to open and reseal envelopes in a manner which cannot readily be detected. Accordingly, care should be taken so as not to reveal classified information in personal correspondence nor to express personal opinions or write on controversial issues which might prove embarrassing to the U.S. Government, the writer or the addressee.

g. Medical or dental service should be obtained only from a U.S. Government facility or from individuals or institutions approved by U.S. Consular Officials. Speech-inducing drugs, medicines, serums and anesthesia are known to have been used under the guise of medical treatment for the purpose of aiding in interrogations. Consideration should be given to the possibility that they might be used in certain circumstances where an enemy may be interested in obtaining highly sensitive information. Normally, the only place where a traveler might be exposed to this type of treatment would be in the private-type clinic or office of a doctor. Except under emergency circumstances, medical treatment or services should not be utilized or sought in Communist or unfriendly areas, other than from the U.S. Embassy.

h. Hotel or other temporary housing should be arranged through U.S. Embassies, or Consulates or military offices. The use of private foreign hotels by travelers exposes them to possible compromise of classified information and possible embarrassment. Traveler's registration is reported to the police. In some areas certain forms are required of hotel guest and such information is then furnished to the police. Often times, the hotel holds a traveler's passport overnight or a short period of time. In those instances, obtain a receipt from the hotel and record your passport number or memorize the number.

i. Under no circumstances should classified information be discussed in housing facilities overseas. No discussion of any type which might prove embarrassing to the U.S. Government should be entered into in any housing facility overseas. Even though classified information may have appeared in the press, do not repeat such information to unauthorized persons or in any public places. Rooms can be monitored and conversations recorded by electronic means without any apparent physical penetration. In many countries luggage and the effects of hotel guests are surreptitiously and thoroughly searched by hotel employees who report to the police, and others.

j. All U.S. travelers in a foreign country are under the technical jurisdiction of the local U.S. Ambassador or the U.S. Consul. A traveler can, and should, contact a U.S. Consulate or Embassy to register his arrival and departure and in the event assistance is required. If a traveler gets in trouble, the Embassy cannot provide a lawyer, but should be expected to be able to recommend where reliable assistance can be obtained.

k. Restrictions vary on the carrying and the use of cameras and portable radios in certain countries or areas. It should be determined in advance the requirements of each country to be visited. Normally the Customs Service of these countries take an interest in such articles, especially if they are new. It is recommended that cameras not be used in "Restricted" areas of both U.S. and foreign countries, and in particular in the Soviet Zone of Germany or the Soviet Sector of Berlin. Usually, U.S. Customs has a service window in the international departure area of airports where a receipt can be obtained for new cameras or other equipment as proof that the article was brought with you from the United States. Carrying of firearms is prohibited.

l. Travelers to, or through, Communist or unfriendly countries and to international and professional meetings where representatives of Communist or unfriendly countries may participate or be in attendance, assume a significant personal and official responsibility as a representative of the United States Government. You may be sure that upon application for a visa to a Communist or unfriendly country particularly, biographical and Intelligence data concerning the traveler is forwarded to the Intelligence office of the country being visited. You will be under constant surveillance while in Communist Bloc countries, with or without your knowledge. Always assume that your actions and remarks while in these areas are being monitored or recorded by intelligent, well-trained agents who know how to exploit the information obtained through various covert and other means.

m. There are two entrapment scenarios which bear mentioning. The first is that in which a traveler is asked by a national in the foreign country being visited, to take a letter or package of personal material to a relative who lives in the United States. The package actually contains incriminating material, often purported to be classified material illegally obtained, and the traveler is apprehended as he takes possession of the item. The second is the illegal exchange of money. This is a classic trouble maker. It is known that travelers have had the experience of a stranger attempting to put money in the traveler's pocket at an airport or on the street, to give the appearance of involvement in illegal money transactions. If successful in "planting" the money, an authority figure steps in and takes the traveler into custody.

n. Each person will conduct himself in such a manner that he cannot be compromised or become involved in any incidents that will embarrass the office he represents.

o. Travelers are specifically instructed that they are not to undertake, or in any manner cause anyone to consider any part of their official travel, an Intelligence operation. Travelers will conduct only that official business for which travel was authorized and in the area of their professional competence.

9-9. Membership in Organizations

a. The NSC poses no objections to your participation in the activities of any reputable organization. You do, however, have the responsibility to determine the policies, stated aims, names of the officers, sponsors and past history of organizations prior to becoming a member, or contributing to, or signing a petition in support of, that organization.

b. In addition to exercising prudence in your choice of organizational affiliations, you should endeavor to avoid participation in public activities of a conspicuously controversial nature, when such activities could focus undesirable attention upon you and, in turn, on the NSC or the White House. NSC personnel may of course participate in bona fide public affairs such as elections or local politics, so long as such activities do not violate the provisions of the statutes and regulations which govern political activity by federal employees.

9-10. Changes in Marital Status and Name Changes

a. All personnel either employed by or assigned to NSC, must advise Security of any changes in their marital status, either through marriage or divorce, or a legal name change.

b. Any intent to marry a person who is not a citizen of the United States must be reported immediately to Security. Marriage to an alien could adversely affect your security clearance.

9-11. Use of Illegal Drugs or Narcotics - It is the policy of the NSC to seek to protect and eliminate the improper use of drugs by employees or other personnel associated with the NSC. The term "drugs" includes all controlled drugs or substances identified and listed in the Controlled Substances Act of 1970, as amended, which includes, but are not limited to, narcotics, depressants, stimulants, hallucinogens and cannabis (marijuana, hashish, and hashish oil). The improper use of drugs by persons employed in, assigned to or detailed to the NSC may adversely affect the national security, may have a serious damaging affect on the user's physical and mental health, may jeopardize the person's safety and the safety of others, and may lead to criminal prosecution.

The improper use of drugs either within or outside NSC controlled facilities is prohibited. The failure of NSC employees and other persons associated with the NSC to observe this policy may constitute grounds for disqualification for initial or continued employment, assignment or detail, or access to classified information or to the White House Complex.

9-12. Leak Investigations - Alleged unauthorized disclosures of classified material are investigated by the Federal Bureau of Investigation (FBI) and it is the policy of the NSC to fully cooperate in these investigations to the greatest degree possible. As a bona fide law enforcement agency, the FBI uses polygraph as an investigative tool. If, during the course of an inquiry into the unauthorized disclosure of classified information, an NSC person is requested by the FBI to submit to a polygraph examination, that person is expected to comply with the request.

9-13. Passes - Control for anyone entering the White House Complex is the responsibility of the United States Secret Service (USSS), Room 23, EOB. The White House Security Office, Room 84, EOB, administers the day-to-day issuance and processing of passes. The USSS has published a booklet entitled "WAVES Center" in which is outlined the methods of making appointments for visitors and various badge/pass procedures. That publication should be referenced for specific procedure. The comments below provide additional information about NSC procedure.

a. Permanent Pass - Permanent passes, either to the White House or the Old Executive Office Building display a color photograph of the passholder. This color photo indicates a full field background investigation has been conducted and the bearer of the pass is eligible for access to Top Secret information on a "need-to-know" basis.

b. White House Pass - There is a specific allocation on the numbers of White House passes that may be issued. That number is controlled jointly by the USSS and the White House Security Office and administered by the NSC Administration Office. White House passholders may escort others in the White House to include providing tours to small numbers of guests.

c. Temporary White House Pass - This pass has a blue border and the letter "T" in the center. It is issued to personnel who are assigned to the West Wing; who are candidates for a permanent White House pass; who have had a favorable FBI namecheck returned, and who are awaiting the completion and favorable evaluation of a full field background investigation.

d. Generic NSC White House Pass - This pass, with a blue border and the letters "NSC" in the center, is for official business use only and is designed to allow holders of an Old Executive Office Building (EOOB) pass to enter the West Wing without an appointment. It is not to be used to provide tours for guests or to give to someone to allow them access into the compound. The pass should not leave the White House Complex.

e. Old Executive Office Building Pass - This gives the passholder access to the Old and the New Executive Office Buildings. To enter the White House, an appointment must be made by a White House passholder.

f. Pass Protection/Display - The pass is a constant reminder of the security requirements that accompany an individual's decision to work in the NSC/White House Complex. The pass should be protected as something of value and if lost, reported immediately to NSC Security, the Administration Office or the USSS. Always display the pass when in the compound, and never display the pass when outside the compound. To display the pass outside the compound is to provide information as to where you work to the general public, and they do not have that "need-to-know."

g. Requirements - When a person is first employed by the NSC or detailed here for an extended period of time, in either the Old Executive Office Building or the White House, they are placed on a 30 day "awaiting pass" list. During this time, a namecheck is requested from the FBI. Upon the return of a favorable report, a temporary picture pass, displaying a black and white photograph of the person is issued. For personnel detailed to the White House Complex for more than three months, the White House Security Office and the USSS require a full field background investigation that is not more than one year old. The NSC also uses that investigation as a basis for special clearances that NSC staff members may require. Upon first arriving for duty at the NSC, an updated set of background investigation forms must be completed and submitted to the NSC Security Office to initiate the FBI investigation. Any delay in submitting the forms will delay completion of the investigation and in turn delay the clearance procedure. Upon receipt of a favorable background investigation, White House Security issues a permanent pass, either for the White House or the EOB, and another government agency issues the necessary clearance. Unfavorable information must be reviewed and evaluated by both the White House Security Office and the other government agency. When all aspects of the background investigation and processing are entirely favorable, the procedure can take as little as two months to complete. Questionable background information will require evaluation by both the agency that issues the clearance and White House Security/USSS on the suitability and eligibility of the individual to have access to the Complex.

h. The sensitivity of working in the White House Complex carries with it extra requirements for suitability and security that exceed the requirements for access to other highly classified areas. Unfavorable background information that might otherwise be acceptable in another secure environment, may not be acceptable for access to the White House Complex.



Information Security Oversight Office
Washington, DC 20405



December 29, 1987

Dear Mr. Stevens:

A last minute rider to the Continuing Resolution for Fiscal Year 1988 (Section 630 of Public Law 100-202, copy enclosed), passed by Congress on December 21, and signed by the President on December 22, 1987, places limitations on the implementation and enforcement of the Standard Form 189, "Classified Information Nondisclosure Agreement." The Information Security Oversight Office (ISOO) will seek an Opinion of the Attorney General on the impact of this legislation on the SF 189 and the SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)." In the interim, and pending further instructions, please implement the following actions at once, including immediate notification to all affected subordinate activities:

1. Cease any additional implementation of existing editions of the SF 189 and SF 189-A. That is, do not have any other personnel execute the August 1983 edition of SF 189, or the June 1986 edition of SF 189-A. ISOO intends to issue as quickly as possible revised editions of each form. You will be provided further instructions as they become available.

2. Do not destroy any existing executed copies of SF 189 and SF 189-A. If at all possible, ISOO will seek to maintain their validity to the extent that they are consistent with the language of Pub. L. 100-202 and revised editions of the forms.

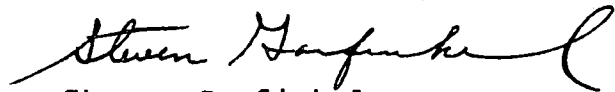
3. Continue the moratorium on any action against a cleared individual who has refused to execute SF 189 in the past. In all likelihood, this moratorium will be lifted when new editions of the nondisclosure agreements are available.

4. Brief cleared unsigned personnel fully on their obligations to protect classified information, and on the sanctions that may result from unauthorized disclosures.

5. Take all appropriate sanctions against personnel who disclose classified information without authority, whether they have signed a nondisclosure agreement or not. Consult with agency counsel, Justice Department counsel, or ISOO concerning the enforceability of executed nondisclosure agreements in taking such actions.

Please contact your ISOO liaison or me at FTS 535-7251 (commercial (202) 535-7251), if you have any questions.

Sincerely,



Steven Garfinkel
Director

The Honorable
Paul Schott Stevens
Executive Secretary
National Security Council
The White House
Washington, DC 20500

Enclosure