

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: 99017-003

Folder Title:
NSC Procedural Manual - Binder 1 [3]

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 Grant Green From: Paul Schott Stevens Re: Request for Access to NSCID 1 and NSDD 207 (1 pp.)	9/10/87	(b)(1)	S
02. Memorandum	For Paul Schott Stevens From: Nancy Menan Re: Request for Access (1 pp.)	8/28/87	(b)(1)	
03. Letter	For Mr Green From: Steven Garfinkel Re: Advisory Notice (3 pp.)	7/6/87	(b)(1)	C
04. Memorandum	For Christopher Hicks From: Robert Kimmitt Re: Security (1 pp.)	4/1/85	(b)(1)	C
05. Paper	Re: US Intelligence Community Physical Security Standards (10 pp.)	n.d.	(b)(1)	
06. Memorandum	For Edward Wilson From: Paul Thompson Re: Security Requirements (1 pp.)	11/1/84	(b)(1)	C
07. Memorandum	For Security Officer From: Technical Security Division Re: Security Survey (3 pp.)	1/18/84	(b)(1)	C
08. Memorandum	For John Brady From: Mary Dix Re: Justification of Sole Source Procurement (1 pp.)	9/26/84	(b)(1)	C
09. Form	Procurement File Copy (1 pp.)	9/26/84	(b)(1)	

Page 1 of 2

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 [3]

Pinksheet Number: MB14496
OA/ID Number: 99017-003
Date Closed: 9/4/2019
FOIA/Sys Case #: 2019-1493-S
Re-review Case #:
P-2/P-5 Review Case #:

Withdrawal/Redaction Sheet

(George Bush Library)

Doc. No. / Type	Subject/Title	Date	Restriction	Classification
10. Memorandum	For Paul Thompson Re: Status of Security Upgrade (2 pp.)	3/7/85	(b)(1)	
11. Memorandum	For Distribution list Re: Promulgation of Policy re Visa Applications for Personnel Assigned to the USSR (2 pp.)	3/27/87	(b)(1)	✓
12. Memorandum	For Robert McFarlane From: Paula Dobriansky Re: Imposition of Travel Restrictions (2 pp.)	12/10/85	(b)(1)	S
13. Memorandum	For Robert McFarlane From: Nicholas Platt Re: Imposition of Travel Restrictions (1 pp.)	12/2/85	(b)(1)	S
14. Paper	Re: NSDD 196 - Counterintelligence/Countermeasure Implementation Task Force (5 pp.)	11/1/85	(b)(1)	S

Page 2 of 2

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 [3]

Pinksheet Number: MB14496
OA/ID Number: 99017-003
Date Closed: 9/4/2019
FOIA/Sys Case #: 2019-1493-S
Re-review Case #:
P-2/P-5 Review Case #:

One Hundredth Congress of the United States of America

AT THE FIRST SESSION

*Began and held at the City of Washington on Tuesday, the sixth day of January,
one thousand nine hundred and eighty-seven*

Joint Resolution

Making further continuing appropriations for the fiscal year
1988, and for other purposes.

Resolved by the Senate and House of Representatives of the
United States of America in Congress assembled,

EMPLOYEE DISCLOSURE AGREEMENTS

630. No funds appropriated in this resolution or any other act for fiscal year 1988 may be used to implement or enforce the agreements in Standard Forms 189 and 4193 of the Government or any other nondisclosure policy, form or agreement if such policy, form or agreement:

(1) concerns information other than that specifically marked as classified; or, unmarked but known by the employee to be classified; or, unclassified but known by the employee to be in the process of a classification determination;

(2) contains the term 'classifiable';

(3) directly or indirectly obstructs, by requirement of prior written authorization, limitation of authorized disclosure, or otherwise, the right of any individual to petition or communicate with Members of Congress in a secure manner as provided by the rules and procedures of the Congress;

(4) interferes with the right of the Congress to obtain executive branch information in a secure manner as provided by the rules and procedures of the Congress;

(5) imposes any obligations or invokes any remedies inconsistent with statutory law.

Provided, that nothing in this section shall affect the enforcement of those aspects of such nondisclosure policy, form or agreement that do not fall within subsections (1)-(5)

of this section

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

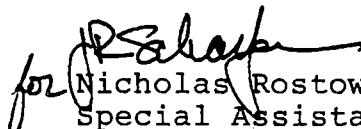
December 17, 1987

MEMORANDUM FOR STEVEN GARFINKEL
Director
Information Security Oversight Office

SUBJECT: NSC Staff Answers to Representative Sikorski's
Questions Submitted to ISOO Regarding SF 189

Enclosed is a copy of our modified answers to Representative Sikorski's questions regarding SF 189. You will note that we have changed our answers to questions II.3 and III.4.

As I indicated in our earlier conversation, only ISOO's answers should be provided to Representative Sikorski.


for Nicholas Rostow
Special Assistant to the President
and Legal Adviser

Attachment

NSC ANSWERS TO QUESTIONS REGARDING STANDARD FORM 189

I. Basis and Need for Nondisclosure Agreements

Question 6: Who in the National Security Council (NSC) authored SF 189? Who in the NSC reviewed and approved the nondisclosure agreement? Who in the Department of Justice reviewed the form before and since its release?

Answer:

The National Security Council (NSC) staff was not the author of SF 189.

National Security Advisor William P. Clark approved SF 189 for the President on August 10, 1983.

II. Implementation of SF 189

Question 2: How many employees without security clearances have signed SF 189? What was the legal authority to require signatures by employees without security clearances? Is this practice still continuing?

Answer:

None.

Question 3: Were Oliver North, Fawn Hall, or William Casey at any time required to sign a nondisclosure agreement? If not, why not? If so, what agreement, and what enforcement actions have been taken, or investigations opened, to hold Messrs. Casey and North and Ms. Hall, accountable for their potential violations of the nondisclosure agreement they signed?

Answer:

LtCol Oliver North and Ms. Fawn Hall signed Standard Form 189s, Classified Information Nondisclosure Agreements, and Form 4193s, Sensitive Compartmental Information Nondisclosure Agreements.

LtCol North has been reassigned to the U.S. Marine Corps and Ms. Hall has been reassigned to the Department of Defense. Activities of LtCol North currently are under investigation by Independent Counsel Walsh.

Question 6: What retraining has the Administration initiated to correspond with all the recent clarifications? Has the retraining been consistently implemented for all agencies and employees covered by SF 189?

Answer:

The NSC has not initiated retraining with respect to SF 189.

Question 7: If there has been no retraining to teach civil servants the impact of the new "clarifying" rules and modifications for SF 189, is any planned? Under what circumstances would additional training be necessary?

Answer:

SF 189 has not created any problems for the NSC staff that merit retraining.

Question 9: Please describe fully the procedures to implement section 1.6(a) of E.O. 12356, under which employees may challenge the status of information that they believe has been improperly classified in order to conceal illegality or other misconduct.

NSC staff members may challenge the status of information they believe has been improperly classified in order to conceal illegality or other misconduct by bringing the information to the attention of the NSC Executive Secretary for classification review under Executive Order 12356. Any allegations of illegality or misconduct would also be brought to the attention of the NSC Legal Adviser and other appropriate authorities as warranted.

Question 10: How many challenges of allegedly improper classifications have been filed under section 1.6(a) of E.O. 12356? How many classification decisions have been upheld and how many have been reversed? What is the range and average times to make decisions under section 1.6(a)?

Answer:

None.

III. Flow of Information to Congress

Question 4: Who determines whether Members of Congress or any other potential recipient has a "need to know" classifiable information and what written criteria or guidelines are applied to make this determination? (Please identify all individuals in all covered agencies, by office name and individual name and title, who have this responsibility.)

Answer:

The policy of this Administration is to comply with Congressional requests for information, including classified information, to the fullest extent consistent with the constitutional and statutory obligations of the Executive branch.

VI. Effect on Employees

Question 4: How many employees have been denied security clearances due in whole or in part to their failure to sign SF 189?

Answer:

None.

Question 5: How many employees have been put on an ineligible list for promotions due in whole or in part to their failure to sign SF 189?

Answer:

None.

VII. Employee Rights

Question 1: What is the range of due process rights for employees at various agencies who face disciplinary action, revocation of security clearance or denial of security clearance for failing to sign SF 189? Please provide legal citations for the appropriate regulations at each covered agency as well as the procedures available for the employee to challenge these three potential consequences.

Answer:

The NSC complies with the relevant provisions, when applicable, of 5 U.S.C. Chapter 75 and 5 C.F.R. Part 752.

Question 1A: Please provide the same information for an employee charged with violating SF 189.

Answer:

The NSC complies with the relevant provisions, when applicable, of 5 U.S.C. Chapter 75 and 5 C.F.R. Part 752.

X. Classification Guide

Question 3: What is the procedure by which users of the Classification Guides may challenge security classifications reflected in the guides?

Answer:

Users of the classification guides may challenge security classifications reflected in the guides by bringing the matter to the attention of the NSC Executive Secretary and the Senior Director for Information Policy/Security Review.

Question 4: Who is the final authority on the proper interpretation and application of a Classification Guide?

Answer:

The NSC Executive Secretary, in consultation with the Senior Director for Information Policy/Security Review and NSC Legal Adviser.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

December 15, 1987

MEMORANDUM FOR STEVEN GARFINKEL
Director
Information Security Oversight Office

SUBJECT: SF 189

Attached is a copy of recent correspondence between Lieutenant General Colin L. Powell and Senator Charles E. Grassley regarding Standard Form 189. Consistent with General Powell's letter, the NSC concurs in ISOO's publication in the Federal Register of the additional clarification of the term "classifiable information."


Paul Schott Stevens
Executive Secretary

Attachment
Tab A Colin Powell Letter to Senator Grassley

THE WHITE HOUSE
WASHINGTON

December 3, 1987

Dear Senator Grassley:

This letter is to inform you that the Information Security Oversight Office (ISOO) will be publishing in the Federal Register a further clarification of the term "classifiable information" as used in Standard Form 189, "Classified Information Nondisclosure Agreement."

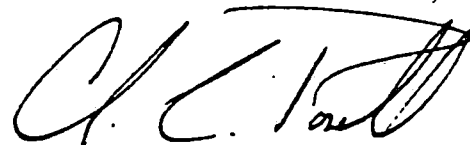
As you know, the term was first used in Standard Form 189 in September 1983. On August 3 and 11, 1987, ISOO published definitions of the term "classifiable information" in the Federal Register in an attempt to clarify its meaning and make clear that the term applies to a very narrow class of information.

Subsequently, at a Post Office and Civil Service Subcommittee hearing on October 15, 1987, you and others in Congress expressed concern about the use of the term "classifiable information." In response to your concerns, representatives of ISOO and the NSC staff met with members of Senator Proxmire's, Senator DeConcini's and your staff in an effort to explore a mutually agreeable formulation.

In this meeting, your staff was provided with a draft of the revised definition, which had been drawn up to reflect changes suggested by your office and in order to satisfy your concerns regarding the use of the term "classifiable information." These changes were derived from Mr. Carlucci's earlier correspondence regarding SF 189; Mr. Carlucci had tried unsuccessfully to reach you by phone to discuss this matter, including the specific clarifying language ISOO will be publishing and including on the Form.

I hope that the clarification ISOO will provide satisfies your concerns regarding SF 189.

Sincerely,



Colin L. Powell
Acting Assistant to the
President for National
Security Affairs

The Honorable Charles E. Grassley
United States Senate
Washington, D.C. 20510

DRAFT

BILLING CODE 6820 KC

INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2003

National Security Information
Standard Forms

AGENCY: Information Security Oversight Office (ISOO)

ACTION: Final Rule.

SUMMARY: This is an amendment to 32 CFR § 2003.20. In recent months, questions have been raised about the intended scope of the term "classifiable information," a term that has been used in the Standard Form 189, "Classified Information Nondisclosure Agreement," since it was first issued in September 1983. On August 3 and 11, 1987, ISOO published definitions of the term "classifiable information" in the Federal Register. These definitions were designed to clarify the meaning of this term and to demonstrate that it applies to a very narrow class of information. Subsequently, it has become evident that further clarification is desirable for purposes of alleviating concern and dispelling confusion about the actual scope of the nondisclosure obligation in regard to such information. Relevant explanatory information circulated by ISOO since August 1987 has proved useful in further clarifying the intended reach of the term "classifiable information." As a result, ISOO has determined that it would be desirable to amend its published definition to incorporate such further explanation. The revised

definition does not change the substance of the term "classifiable information" in each executed nondisclosure agreement, but may, nevertheless, prove useful to a better understanding by affected employees of their nondisclosure obligations. While ISOO will include this definition in future reprints of the Standard Form 189, it is intended to apply to all editions of the Form.

EFFECTIVE DATE: Upon Publication.

FOR FURTHER INFORMATION CONTACT:

Steven Garfinkel, Director, ISOO.

Telephone: (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.

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 (h)(1) is revised to read as follows:

(h) * * *

(1)(i) As used in paragraph 1 of SF 189, the term "classifiable information" refers to two categories of information only: (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.

"Classifiable information" does not refer to currently unclassified information that may be subject to possible classification at some future date, but is not currently in the process of a classification determination. Therefore, the only circumstances under which a party to SF 189 might violate its terms 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.

DRAFT

(ii) A party to SF 189 may be liable for disclosing "classifiable information" only 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 to SF 189 be liable for violating its 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.

Dated:

Steven Garfinkel
Director, Information
Security Oversight Office

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

December 10, 1987

ACTION

MEMORANDUM FOR PAUL SCHOTT STEVENS

FROM:

for NICHOLAS ROSTOW *NR*

SUBJECT:

SF 189

Attached at Tab I is a memorandum from you to Steve Garfinkel, Director of Information Security Oversight Office. Your memorandum forwards a copy of General Powell's letter to Senator Grassley announcing our intention to publish in the Federal Register a further clarification of the term "classifiable information" as used in Standard Form 189. In connection with General Powell's letter, your memorandum directs Mr. Garfinkel to initiate this publication.

not available
Dave Matthews concurs.

RECOMMENDATION

That you sign the memorandum at Tab I.

Approve

DM

Disapprove _____

Attachments

Tab I - Stevens Memorandum to Garfinkel

Tab A - Powell Letter to Grassley, December 3, 1987

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

September 10, 1987

Dear Mr. Holmes:

In response to your letter of July 14, 1987, I am forwarding to you a copy of the unclassified National Security Council Intelligence Directive 1, dated February 17, 1972, and entitled "Basic Duties and Responsibilities."

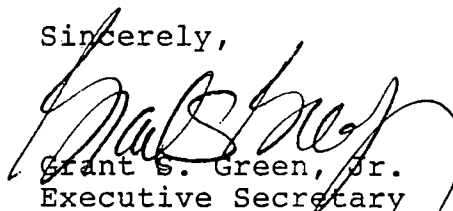
We will be happy to provide the NSDD for your review, subject to the following conditions:

- We request certification that the staff member holds the requisite security clearance.
- The document will be available at the NSC for your staff to review. If you wish to read the document personally, I will arrange to have a staff officer meet with you for that purpose.
- No copy of the document may be made.
- Any notes taken concerning the document must be handled as classified information and reviewed by the NSC staff prior to transmittal.
- Portions of any resulting report citing classified NSC material should be submitted to the NSC staff for review prior to publication.

Please call Brenda Reger at 395-3736 to arrange a time to review the document.

Additionally, D. Barry Kelly, of the NSC staff, would be pleased to provide briefings on request. If you are interested in receiving a briefing, please contact Alison Fortier, Special Assistant to the President and Senior Director of Legislative Affairs, to make arrangements. Her phone number is 395-4682.

Sincerely,



Grant S. Green, Jr.
Executive Secretary

Attachment: NSCID 1

The Honorable Sven E. Holmes
Staff Director and General Counsel
U.S. Senate Select Committee on Intelligence
Washington, DC 20510-6475

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
01. Memorandum	For Grant Green From: Paul Schott Stevens Re: Request for Access to NSCID 1 and NSDD 207 (1 pp.)	9/10/87	(b)(1)	S

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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

5445

DAVID L. BOREN, OKLAHOMA, CHAIRMAN
WILLIAM S. COHEN, MAINE, VICE CHAIRMAN

LLOYD BENTSEN, TEXAS
SAM NUNN, GEORGIA
ERNEST F. HOLLINGS, SOUTH CAROLINA
BILL BRADLEY, NEW JERSEY
ALAN CRANSTON, CALIFORNIA
DENNIS DECONCINI, ARIZONA
HOWARD M. METZENBAUM, OHIO

WILLIAM V. ROTH, JR., DELAWARE
ORRIN HATCH, UTAH
FRANK MURKOWSKI, ALASKA
ARLEN SPECTER, PENNSYLVANIA
CHIC HECHT, NEVADA
JOHN WARNER, VIRGINIA

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-8475

ROBERT C. BYRD, WEST VIRGINIA, EX OFFICIO
ROBERT DOLE, KANSAS, EX OFFICIO

SVEN E. HOLMES, STAFF DIRECTOR/GENERAL COUNSEL
JAMES H. DYKSTRA, MINORITY STAFF DIRECTOR
KATHLEEN P. MCGHEE, CHIEF CLERK

July 14, 1987

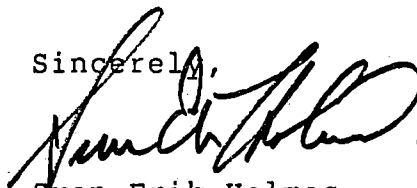
Mr. Grant S. Green, Jr.
Executive Secretary
National Security Council
Washington, D.C. 20506

Dear Mr. Green:

It is requested that the Senate Select Committee on
Intelligence be provided a copy of:

NSCID 1
NSDD 207

Sincerely,



Sven Erik Holmes
Staff Director

SEH:cb

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

August 28, 1987

MEMORANDUM FOR PAUL SCHOTT STEVENS

FROM: NANCY V. MENA *Am*

SUBJECT: SSCI Request for Access to NSDD 207

I do not concur on this action for the following reasons:

Past practice has been to accept requests for access to NSDDs from either the committee chairman OR the staff director. Therefore, a response from us requiring a request from the SSCI chairman might easily be viewed as a convenient change in practice.

Of note, although the original version of the NSDD is TOP SECRET, a sanitized version, downgraded to SECRET, was done in response to a FEMA request in April, 1986. The number and title together are now SECRET, not TS.

I have no objection to a briefing nor access to the SECRET version of NSDD 207 subject to our standard procedures.

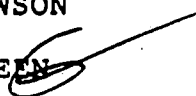
*Package rewritten to reflect
the above
JRS*

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

Dix

September 1, 1987

MEMORANDUM FOR RHETT DAWSON

FROM: GRANT GREEN 

SUBJECT: NSC Security/Space

As a result of findings and the recommendations made by the Tower Board, the National Security Council is taking steps to upgrade overall security within the organization. In addition to improving personnel security awareness and procedures, major steps will be required to upgrade physical security -- particularly that associated with the preservation and maintenance of classified documents. The latter includes sensitive/restricted intelligence material and Presidential records as well as all other documents related to the enhancement and continuity of national security records management.

The first major project to be undertaken will be the renovation of the Secretariat which occupies Rooms 377 to 387 in the OEGB. The volume of the documents that the Secretariat controls, dictates that we must maintain an "open storage" configuration in the storage vault area (Room 377). The security condition of this space has been marginal for many years. However, with renovation, the area can be upgraded to meet established security/intelligence community standards. Specific improvements will include reinforcing one wall with hardened steel plate, installing a bank vault door, manproofing the windows, and improving access control hardware. In addition, another portion of the Secretariat must be reconfigured into a special "limited access" facility. This modification -- required to enhance the administrative processing and storage of sensitive files relocated from other staff offices -- will also require special security treatment to ensure compartmentation and access control.

The above requirements represent an additional investment in dollars, space and people. In that the present configuration of the Secretariat does not include adequate space to accommodate the new files and additional staff, there appear to be two alternatives: (1) Double-deck a relatively small area within the Secretariat or (2) identify additional space in the Old Executive Office Building which would meet, or could be upgraded, to security standards.

I would appreciate your thoughts on the above.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

5818

August 10, 1987

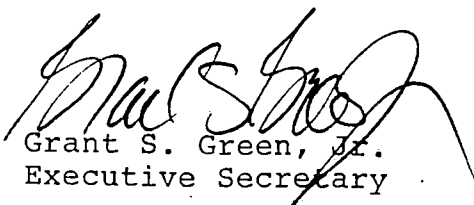
MEMORANDUM FOR STEVEN GARFINKEL

Director, Information Security Oversight Office

SUBJECT: Classified Information Nondisclosure Agreement

We recommend that you take the following actions pertinent to the Standard Form 189, "Classified Information Nondisclosure Agreement," and Standard Form 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)." These changes are intended solely to clarify what some have called ambiguities. They are consistent with the Administration's interpretation of these provisions and have no substantive impact upon the terms of the nondisclosure agreements.

- (1) That you amend 32 CFR Part 2003, "National Security Information; Standard Forms":
 - (a) To provide a definition of the term "classifiable" as it appears in paragraph 1 of the SF 189 that is consistent with the definition that your office has used in its written explanations of the term;
 - (b) To clarify that the first sentence of paragraph 7 of the SF 189 refers to classified information exclusively;
 - (c) To clarify that the third and fourth sentences of paragraph 7 of the SF 189 and SF 189-A refer to classified materials exclusively;
 - (d) To clarify that the third sentence of paragraph 7 of the SF 189 and SF 189-A should read: "... materials which have or may come into my possession..."
- (2) That upon the publication of these clarifications in the Federal Register, you notify each affected agency of them; and
- (3) That upon the reprinting of the SF 189 and SF 189-A, the clarifications outlined in paragraphs (1)(b), (c) and (d), above, be reflected in the language of the forms.


Grant S. Green, Jr.
Executive Secretary



Information Security Oversight Office
Washington, DC 20405

5818

July 14, 1987

MEMORANDUM FOR: David Major
National Security Council

FROM: Steven Garfinkel *Steve Garfinkel*
Director, Information Security Oversight Office

SUBJECT: Classified Information Nondisclosure Agreement

I enclose for your information correspondence to and from the Information Security Oversight Office (ISOO) regarding the Standard Form 189, "Classified Information Nondisclosure Agreement," that has ensued since we submitted on July 2, a draft response to Chairman Sikorski's letter to Mr. Carlucci dated June 24. I especially call to the NSC's attention the correspondence from Chairwoman Schroeder of the Subcommittee on Civil Service. It is my understanding that Mr. Sikorski has indicated his interest in holding joint hearings with her on the SF 189. It is clear from Mrs. Schroeder's letter of July 13, that she is not particularly inclined to make a major issue of this one-man controversy. She seems prepared to drop the matter if ISOO takes the regulatory steps that we proposed in my letter to her of July 13, and suggested in our draft response to Mr. Sikorski.

Under these circumstances, I believe that it is critical that we act promptly and affirmatively to help defuse this issue by making the non-substantive regulatory clarifications that we have proposed. I also believe that it would be most beneficial if the direction to ISOO to proceed with these regulatory changes comes from the NSC. To that end, I enclose a draft of a memorandum from the Staff Secretary to me requesting this action and copies of the SF 189 and 189-A.

Enclosures



Information Security Oversight Office
Washington, DC 20405

July 10, 1987

Dear Mr. Kolesnik:

This follows up on our telephone conversation yesterday afternoon about the Standard Form 189, "Classified Information Nondisclosure Agreement." I appreciate the opportunity to express directly the views of the Information Security Oversight Office (ISOO), which is responsible for issuing and overseeing executive branch implementation of the nondisclosure agreement, rather than being "quoted" by third parties. I also appreciate from our conversation that our goals are largely the same, even if we do not yet agree on how to achieve them. As I note below, however, I believe that there are reasonable, alternative means of resolving these differences that do not require the suspension of the SF 189.

The executive branch requires the execution of this nondisclosure agreement for two reasons. First, it alerts employees of the trust that is placed in them by providing them access to classified information and of their responsibilities to protect that information from unauthorized disclosure. Second, it states in standard, written terms the nature of that trust and those responsibilities, so if that trust is violated, the United States will be in a far better position to enforce the agreement.

The terms of the SF 189 are less stringent than those of other nondisclosure agreements which the Federal courts, including the Supreme Court, have consistently validated. Four years ago, when its language was first drafted, constitutional experts at the Department of Justice reviewed every provision. Before it was issued, several committees of Congress and representatives of the American Civil Liberties Union and other public interest organizations scrutinized the form. No legal action against the nondisclosure agreement resulted. Since then, approximately two million civilian and military personnel, including our top officials, have signed the SF 189, and thousands more are being signed each day. This has been accomplished with a minimal amount of controversy and disruption.

As an enclosure, I address in greater detail the three issues for which you requested ISOO's point of view: the meaning of the term "classifiable" as used in paragraph 1 of the SF 189, and why it is not used in the SF 189-A, the nondisclosure agreement designed for Government contractor employees and other non-Government personnel; the absence of the modifier, "classified," before the word "information" in the first sentence of paragraph 7 of the SF 189, although it appears in the same provision of the SF 189-A; and the relationship of the SF 189 to the so-called "whistleblower" statute, 5 U.S.C. § 2302.

While a few persons have suggested that there are conflicts or discrepancies within these provisions, I believe that, at worst, there are ambiguities that can be resolved far less drastically than through the suspension of the SF 189. For example, under Executive Order 12356, "National Security Information," ISOO issues directives or regulations that have Government-wide application. ISOO could issue a regulatory provision that states explicitly that "information" in paragraph 7 of the SF 189 refers exclusively to "classified information." Further, ISOO could include within this regulation a definition of "classifiable" that would express authoritatively the limits of its application.

On the other hand, suspending the SF 189 would unnecessarily void four years and millions upon millions of dollars of effort. It would halt a worthwhile program a few steps short of its completion. Finally, it would send out a most regrettable message: that the unlawful disclosure of our nation's secrets is lesser threat than a few semantic ambiguities in a lawful agreement designed to help prevent these disclosures.

I also enclose a copy of ISOO's most recent Report to the President. It provides an overview of what ISOO is and what it does. It also includes at Appendix B, page 35, a progress chart, as of the end of FY 1986, on agency by agency implementation of the SF 189. This chart reflects that 70% of the agencies had achieved 100% implementation by that time. Since then, we are much closer to achieving 100% compliance in every agency.

Sincerely,

(Signed) Steven Garfinkel

Steven Garfinkel
Director

Mr. Kris Kolesnik
Office of Senator Charles E. Grassley
United States Senate
Washington, DC 20510

Enclosures

PATRICIA SCHROEDER, COLORADO, CHAIRWOMAN

STEPHEN J. SOLARZ, NEW YORK
WILLIAM B. CLAY, MISSOURICHARLES PASHAYAN, JR., CALIFORNIA
FRANK HORTON, NEW YORK

U.S. House of Representatives

COMMITTEE ON POST OFFICE AND CIVIL SERVICE

SUBCOMMITTEE ON CIVIL SERVICE

122 CANNON HOUSE OFFICE BUILDING

Washington, DC 20515

TELEPHONE (202) 225-4025



July 6, 1987

Mr. Steven Garfinckel
Director
Information Security Oversight Office
General Services Administration
Washington, D. C. 20405

Dear Mr. Garfinckel:

As you know, the Subcommittee on Civil Service devoted considerable attention in 1983 and 1984 to examining Administration efforts to strengthen secrecy agreements following the issuance of National Security Decision Directive 84. As a result of discussions with Administration officials, the Administration clarified its intention with regard to pre-publication review and non-disclosure.

I was, therefore, shocked to read the attached letter signed by Congressman Sikorski and quoting you extensively. What you are quoted as saying is in direct conflict with my understanding of the way our discussions ended.

On page 2, you are quoted as saying that "classifiable" information "could be anything." As I remember our discussions a few years ago, the purpose of this provision was to tell the Federal worker that information which he or she should know is classified, but which through clerical error is not so marked, should not be disclosed. Any broader interpretation is intolerable.

On the bottom of page 2, the Sikorski letter says that you would not direct agencies to amend paragraph 7 of Standard Form 189 to add the qualifier "classified". Is this true? I do not understand why you would resist making such a change since the clear intent of the words is to apply to classified information only.

On page 4, the letter states that you suggested that SF-189 could be used as a basis for pre-publication review. The agreement struck on this issue was quite clear and it is reflected in Justice Department regulations. Only those non-disclosure agreements which contain explicit pre-

Mr. Steven Garfinckel
July 6, 1987
Page Two

publication review requirements may be used to mandate pre-publication review. Is this not your understanding of the law on this?

I hope you were misquoted in the Sikorski letter. The Subcommittee on Civil Service worked with the National Security Council in 1982 and 1983 to limit pre-publication review to non-disclosure agreements related to Sensitive Compartmented Information. While the new wording of Standard Form 189 is clearly overbroad and vague, it should not be interpreted to permit prosecution in the case of information not known to the employee to be classified. And clearly, nothing in Standard Form 189 contemplates a pre-publication review requirement. I urge you to utilize this opportunity to set the record straight on Standard Form 189 and the circumstances under which a prosecution for its violation would be considered.

With kind regards,

Sincerely yours,

A handwritten signature in cursive script, appearing to read "Pat Schroeder".

PATRICIA SCHROEDER
Chairwoman

enc.

"CLASSIFIABLE" INFORMATION

"Classifiable" refers to information that meets all the tests for classified information under Executive Order 12356, "National Security Information," but which, as a result of negligence, time constraints, error, lack of opportunity or oversight, has not been marked as classified information. A person would violate the agreement if he disclosed without authorization information that he knew, or reasonably should have known, was classified, although it had not yet been marked as such. For example, a person attending a classified meeting should reasonably know that his unmarked notes of that meeting may not be disclosed to a person who doesn't have a clearance and a "need-to-know" that information.

"Classifiable" information, as defined above, has long been a particular concern of the Intelligence Community. This term or similar terms have appeared in nondisclosure agreements used by intelligence agencies for many years preceding its inclusion in the SF 189. In testimony before a Senate subcommittee studying National Security Decision Directive 84, which mandated the creation of a standardized classified information nondisclosure agreement, former CIA Director William Colby alluded to the fact that raw intelligence data are often unmarked as classified when they are first received. The collection of raw intelligence often occurs in circumstances that do not permit the formalities of classification markings. Nevertheless, this intelligence often involves some of the most sensitive information within the Government, such as the names of intelligence sources.

Also, with respect to the term "classifiable," the question has been raised about a person being sanctioned for violating the nondisclosure agreement by disclosing information that was clearly unclassified at the time of disclosure, but was classified subsequent to the disclosure. In almost every hypothetical fact pattern, the prior disclosure would not be a violation of the SF 189. However, it is possible to construct a hypothetical in which it may be. For example, suppose an employee has been informed by his supervisor, who is not an authorized original classifier, that particular unclassified information has been referred to an original classifier for classification action. If the information is classified as a result of this referral, the employee would very likely violate the agreement should he disclose it without authorization in the interim. Because we can hypothesize fact patterns such as this, we cannot state conclusively that the disclosure of unclassified information would never amount to a violation of the SF 189.

CLARITY OF LANGUAGE IN PARAGRAPH 7 OF THE SF 189

The first line of paragraph 7 of the SF 189 reads: "I understand that all information to which I may obtain access by signing this form is now and will forever remain the property of the United States Government." The SF 189-A* includes the word "classified" before the word "information." It has been suggested by a few persons that the SF 189, therefore, imposes a much broader standard.

To the contrary, the first sentences of both agreements mean precisely the same thing, and refer only to classified information. Information to which someone "may obtain access by signing [the SF 189]" is, by definition, classified information. As further stated in the first sentence of the agreement: ". . . I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information." [Emphasis added.] The drafters of the SF 189 did not include the word "classified" in the first sentence of paragraph 7 because they believed it to be redundant. The information referenced in paragraph 7 could only be classified information.

When the SF 189-A was being drafted, the Department of Defense (DoD) requested that the word "classified" be inserted before the word "information" in paragraph 7, notwithstanding its redundancy. DoD sought its inclusion in order to preclude any possibility whatsoever of misunderstanding. Although ISOO initially objected on the basis that its inclusion was unnecessary, it eventually conceded to DoD's request, believing that no harm could result from a simple redundancy. Since reading the forms SF 189 and SF 189-A in tandem has led some to the incorrect suggestion that paragraph 7 of the SF 189 refers to more than just "classified information," ISOO probably should not have made this concession.

*The SF 189-A is the classified information nondisclosure agreement form composed and issued three years after the SF 189 as an adaptation for non-Government employees such as contractor personnel.

CLARITY OF LANGUAGE IN PARAGRAPH 7 OF THE SF 189

The first line of paragraph 7 of the SF 189 reads: "I understand that all information to which I may obtain access by signing this form is now and will forever remain the property of the United States Government." The SF 189-A, composed over three years later, includes the word "classified" before the word "information." It has been suggested by a few persons that the SF 189, therefore, imposes a much broader standard.

To the contrary, the first sentences of both agreements mean precisely the same thing, and refer only to classified information. Information to which someone "may obtain access by signing [the SF 189]" is, by definition, classified information. As further stated in the first sentence of the agreement: ". . . I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information." [Emphasis added.] The drafters of the SF 189 did not include the word "classified" in the first sentence of paragraph 7 because they believed it to be redundant. The information referenced in paragraph 7 could only be classified information.

When the SF 189-A was being drafted, the DoD requested that the word "classified" be inserted before the word "information" in paragraph 7, notwithstanding its redundancy. DoD sought its inclusion in order to preclude any possibility whatsoever of misunderstanding. Although ISOO initially objected on the basis that its inclusion was unnecessary, it eventually conceded to its inclusion believing that no harm could result from a simple redundancy. Since reading the forms SF 189 and SF 189-A in tandem has led some to the incorrect suggestion that paragraph 7 of the SF 189 refers to more than just "classified information," ISOO probably should not have made this concession.

The third sentence of paragraph 7 reads in part: "I agree that I shall return all materials which have, or may have, come into my possession or for which I am responsible because of such access" For the same reasons addressed above, it is clear that "all materials," by definition, refers only to "classified" materials. It is far less clear what is meant by the phrase, "or may have." The current language of this phrase was suggested by the Department of Justice after the interagency drafting group had completed its work on what was to become the SF 189. A detailed review of the records also reveals that the Department suggested slightly different, but far clearer language for the comparable provision of a standardized Sensitive Compartmented Information Nondisclosure Agreement that was later withdrawn by

the White House: "I agree that I shall return all materials which have or may come into my possession or for which I am responsible because of such access" It now appears that Justice intended that the phrase "may have come" should actually have read "may come" in what was to become the SF 189 as well.

At worst, these phrases are simply troublesome ambiguities. They can be clarified by modifying the ISOO regulation implementing the SF 189 and SF 189-A, or by ISOO issuing a clarification letter to all agencies.

CONFLICT WITH "WHISTLEBLOWER" STATUTES

The SF 189 does not conflict with the so-called "whistleblower" statutes (5 U.S.C. § 2302). These statutes specifically do not protect persons who disclose classified information without authorization. The reference in these statutes to information "specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs" is without question a reference to the contemporary Executive order on national security information, which is now E.O. 12356. In turn, SF 189 defines classified information as "information that is either classified or classifiable 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."

In addition, E.O. 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 Executive 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. 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.

The viability of the security classification system depends entirely upon the commitment of cleared persons to protect national security information. If anyone could change an unauthorized disclosure to an authorized disclosure simply by claiming to be a "whistleblower," there would be no system at all to protect the nation's secrets.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information that is either classified or classifiable 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. 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 and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me a security clearance that such disclosure is permitted. 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 and am aware 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; and 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 and am aware 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 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 information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. 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 materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance. 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.
10. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, Section 783(b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, and Executive Order 12356, so that I may read them at this time, if I so choose.
11. I make this Agreement without mental reservation or purpose of evasion.

SIGNATURE	DATE	SOCIAL SECURITY NO. (See notice below)

ORGANIZATION

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to classified information.

WITNESS AND ACCEPTANCE:

SIGNATURE	DATE

ORGANIZATION

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.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information that is either classified or classifiable 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. 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 and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me a security clearance that such disclosure is permitted. 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 and am aware 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; and 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 and am aware 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 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 information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. 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 materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance. 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.

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

11. I make this Agreement without mental reservation or purpose of evasion.

SIGNATURE	DATE	SOCIAL SECURITY NO. (See notice below)

ORGANIZATION

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to classified information.

WITNESS AND ACCEPTANCE:

SIGNATURE	DATE

ORGANIZATION

NOTE: 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.

**CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT
(INDUSTRIAL/COMMERCIAL/NON-GOVERNMENT)**

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Type or print)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information 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. 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 and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or 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 that such disclosure is permitted. 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 and am aware that any breach of this Agreement may result in the termination of any security clearances I hold and removal from any position of special confidence and trust requiring such clearances. In addition, I have been advised and am aware 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, and 798, Title 18, 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 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 forever remain the property of the United States Government. 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 materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or 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)

**CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT
(INDUSTRIAL/COMMERCIAL/NON-GOVERNMENT)**

I AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Type or print)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information 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. 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 and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or 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 that such disclosure is permitted. 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 and am aware that any breach of this Agreement may result in the termination of any security clearances I hold and removal from any position of special confidence and trust requiring such clearances. In addition, I have been advised and am aware 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, and 798, Title 18, 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 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 forever remain the property of the United States Government. 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 materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or 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)

THE WHITE HOUSE
WASHINGTON

July 23, 1987

Leah S
4736
Please file

Dear Congressman Sikorski:

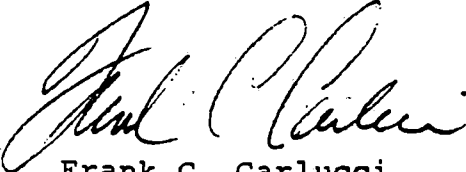
Thank you for your letter of June 24, in which you express some concerns about the Standard Form 189, "Classified Information Nondisclosure Agreement." Please be assured that we appreciate your viewpoint and have considered your recommendations carefully. However, we are convinced that this nondisclosure agreement fulfills a very important national security purpose and that it deprives no one of rights guaranteed under the Constitution and laws of the United States. As an enclosure to this letter, we address your major concerns in greater detail.

National Security Decision Directive (NSDD) Number 84 established the requirement that "all persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." The request for execution of this nondisclosure agreement is for two reasons. First, it alerts employees to the trust that is placed in them by providing them access to classified information and of their responsibilities to protect that information from unauthorized disclosure. Second, it states in standard, written terms the nature of that trust and those responsibilities, so that if that trust is violated, the United States will be in a far better position to enforce the agreement.

The terms of the SF-189 are less stringent than those of other nondisclosure agreements which the Federal courts, including the Supreme Court, have consistently validated. Four years ago, when its language was first drafted, constitutional experts at the Department of Justice reviewed every provision. Before it was issued, several committees of Congress and representatives of the American Civil Liberties Union and other public interest organizations scrutinized the form. No legal action against the nondisclosure agreement resulted. Since then, approximately two million civilian and military personnel, including our top officials, have signed the SF-189, and thousands more are being signed each day. This has been accomplished with a minimal amount of controversy and disruption.

As a result of your letter, we are asking the Director of the Information Security Oversight Office (ISOO) to issue to all agencies an instruction that clarifies some of the ambiguous language in paragraph 7 of the SF-189. The ISOO Director and his staff have been available to respond to questions and concerns about the SF-189 since its inception. He would be happy to meet with you or your staff at your convenience to discuss your concerns.

Sincerely,



Frank C. Carlucci

Enclosures

The Honorable Gerry Sikorski
Chairman, Subcommittee on Human Resources
Committee on Post Office and Civil Service
House of Representatives
Washington, D.C. 20515

PATRICIA SCHROEDER, COLORADO, CHAIRWOMAN
STEPHEN J. SOLARZ, NEW YORK CHARLES PASHAYAN, JR., CALIFORNIA
WILLIAM (BILLY) CLAY, MISSOURI FRANK HORTON, NEW YORK

U.S. House of Representatives

COMMITTEE ON POST OFFICE AND CIVIL SERVICE

SUBCOMMITTEE ON CIVIL SERVICE

122 CANNON HOUSE OFFICE BUILDING

Washington, DC 20515

TELEPHONE (202) 225-4025

July 13, 1987

Mr. Steven Garfinkel
Director
Information Security Oversight Office
Washington, D.C. 20405

Dear Mr. Garfinkel:

Thank you for your letter of today clarifying the intention behind the Classified Information Nondisclosure Agreement, Standard Form 189.

Attached to your letter were three enclosures: one defining the term "classifiable information; another explaining the language differences between SF 189, for Federal employees, and SF 189-A, for contract employees; and another stating that pre-publication review is not required under SF-189. These enclosures interpret SF 189 in a manner consistent with my understanding of the intention of the form.

Your letter states that the ambiguities in SF 189 can be remedied through a directive issued by your office. I urge you to issue such a directive containing the same interpretations as are contained in the enclosures to your letter. While I agree with you that it would not be prudent to attempt to get two million employees to execute new forms without the ambiguous language, I recommend that a new form be issued to be signed by new employees. If these recommendations were adopted, new employees would sign a new nondisclosure agreement which is clear as to what is covered. Pre-existing employees would be subject to existing form SF 189, as clarified by the regulations which you said your office could issue.

I truly appreciate your efforts to clarify the meaning of the Classified Information Nondisclosure Agreement. Please inform me as to what steps you take as a result of this.

With kind regards,

Sincerely yours,



PATRICIA SCHROEDER
Chairwoman



Information Security Oversight Office
Washington, DC 20405

July 13, 1987

Dear Madam Chairwoman:

Thank you for your letter of July 6, concerning the Standard Form 189, "Classified Information Nondisclosure Agreement." I very much appreciate the opportunity to express directly the views of the Information Security Oversight Office (ISOO), which is responsible for issuing and overseeing executive branch implementation of the nondisclosure agreement, rather than being "quoted" by third parties. Please be assured that your understanding of the issues that you raise from Chairman Sikorski's letter remain as we understood them when the Subcommittee on Civil Service reviewed the SF 189 in 1983. I address these issues as an attachment to this letter.

Since we last discussed the SF 189, approximately two million civilian and military personnel have executed it, and thousands more are signing the agreement each day. As of the end of FY 1986, 70% of the agencies that create or handle national security information reported 100% compliance with the requirement to have all cleared personnel sign either the SF 189 or an alternative nondisclosure agreement approved by the National Security Council. Since then, we are much closer to achieving 100% compliance in every agency. We have accomplished this mammoth task with a minimal amount of controversy and disruption.

While a few persons have suggested that there are conflicts or discrepancies within certain provisions of the SF 189, I believe that, at worst, there are ambiguities that can be resolved rather easily. For example, under Executive Order 12356, "National Security Information," ISOO issues directives or regulations that have Government-wide application. ISOO could issue a regulatory provision that states explicitly that "information" in paragraph 7 of the SF 189 refers exclusively to "classified information." Further, ISOO could include within this regulation a definition of "classifiable" that would express authoritatively the limits of its application.

On the other hand, taking a drastic step such as suspending the SF 189 would unnecessarily void four years and millions upon millions of dollars of effort. It would halt a worthwhile program a few steps short of its completion. Finally, it would send out a most regrettable message: that the unlawful disclosure of our nation's secrets is a lesser threat than a few semantic ambiguities in a lawful agreement designed to help prevent these disclosures.

I look forward to working with you and your staff to seek reasonable solutions to any problems that may exist within the nondisclosure agreement program.

Sincerely,

(Signed) Steven Garfinkel

Steven Garfinkel
Director

The Honorable
Patricia Schroeder
Chairwoman
Subcommittee on Civil Service
Committee on Post Office
and Civil Service
U. S. House of Representatives
Washington, DC 20515

Enclosures

"CLASSIFIABLE" INFORMATION

"Classifiable" refers to information that meets all the tests for classified information under Executive Order 12356, "National Security Information," but which, as a result of negligence, time constraints, error, lack of opportunity or oversight, has not been marked as classified information. A person would violate the agreement if he disclosed without authorization information that he knew, or reasonably should have known, was classified, although it had not yet been marked as such. For example, a person attending a classified meeting should reasonably know that his unmarked notes of that meeting may not be disclosed to a person who doesn't have a clearance and a "need-to-know" that information.

"Classifiable" information, as defined above, has long been a particular concern of the Intelligence Community. This term or similar terms have appeared in nondisclosure agreements used by intelligence agencies for many years preceding its inclusion in the SF 189. In testimony before a Senate subcommittee studying National Security Decision Directive 84, which mandated the creation of a standardized classified information nondisclosure agreement, former CIA Director William Colby alluded to the fact that raw intelligence data are often unmarked as classified when they are first received. The collection of raw intelligence often occurs in circumstances that do not permit the formalities of classification markings. Nevertheless, this intelligence often involves some of the most sensitive information within the Government, such as the names of intelligence sources.

Also, with respect to the term "classifiable," the question has been raised about a person being sanctioned for violating the nondisclosure agreement by disclosing information that was clearly unclassified at the time of disclosure, but was classified subsequent to the disclosure. In almost every hypothetical fact pattern, the prior disclosure would not be a violation of the SF 189. However, it is possible to construct a hypothetical in which it may be. For example, suppose an employee has been informed by his supervisor, who is not an authorized original classifier, that particular unclassified information has been referred to an original classifier for classification action. If the information is classified as a result of this referral, the employee would very likely violate the agreement should he disclose it without authorization in the interim. Because we can hypothesize fact patterns such as this, we cannot state conclusively that the disclosure of unclassified information would never amount to a violation of the SF 189.

At the suggestion of the Department of Defense (DoD), the SF 189-A was developed three years after the issuance of the SF 189 to facilitate the execution of nondisclosure agreements among non-Government personnel who require access to classified information. The DoD implements the Defense Industrial Security Program (DISP), which establishes standards for and oversees the maintenance of classified information within industry, both for the DoD itself and for approximately 18 other executive branch agencies that subscribe to the DISP. In drafting the SF 189-A, ISOO sought to revise only those provisions in which the differences between the respective standing of Government and contractor employees, vis-a-vis classified information, warranted modifications. For example, ISOO excluded from the SF 189-A a reference to a criminal statute that listed only Government employees as potential violators.

The reference to "classifiable" information in paragraph 1 of the SF 189 was omitted from the SF 189-A because contractors do not have the authority to classify information originally. All contractor classification actions should result from instructions provided explicitly by an authorized original classifier from within the contracting agency. It is the Government's responsibility to designate, as explicitly as possible, what information is classified and what information is not classified in the performance of a classified contract. As the DoD suggested to ISOO, contractor employees could very reasonably object to the inclusion of the word "classifiable" because it suggests discretion where no discretion exists, i.e., the classification of information by industry.

Although ISOO still had some reservations about deleting the term "classifiable" from the SF 189-A, another important factor ultimately led to its decision to do so. As noted above, concern over "classifiable" information is most prominent within the Intelligence Community. Contractor employees of both the Central Intelligence Agency and the National Security Agency are required to sign nondisclosure agreements that are more stringent than either the SF 189 or the SF 189-A, and these agreements contain references to "classifiable" information or similar terms that go beyond the mere reference to "classified information." This fact convinced ISOO that it was reasonable to delete the term "classifiable" from the SF 189-A, and the Department of Justice, in an enforceability review of the draft form, concurred.

The third sentence of paragraph 7 reads in part: "I agree that I shall return all materials which have, or may have, come into my possession or for which I am responsible because of such access" For the same reasons addressed above, it is clear that "all materials," by definition, refers only to "classified" materials. It is far less clear what is meant by the phrase, "or may have." The current language of this phrase was suggested by the Department of Justice after the interagency drafting group had completed its work on what was to become the SF 189. A detailed review of the records also reveals that the Department suggested slightly different, but far clearer language for the comparable provision of a standardized Sensitive Compartmented Information Nondisclosure Agreement that was later withdrawn by the White House: "I agree that I shall return all materials which have or may come into my possession or for which I am responsible because of such access" It now appears that Justice intended that the phrase "may have come" should actually have read "may come" in what was to become the SF 189 as well.

At worst, these phrases are simply troublesome ambiguities. They can be clarified by modifying the ISOO regulation implementing the SF 189 and SF 189-A, or by ISOO issuing a clarification letter to all agencies.

PREPUBLICATION REVIEW

The SF 189 contains no requirement for prepublication review. This omission resulted from the specific design of its drafters, since NSDD-84 was silent on the inclusion or non-inclusion of a prepublication review provision for this nondisclosure agreement.

The ability of the Government to seek injunctive relief to prevent the publication of classified information is not an implied imposition of a blanket prepublication requirement. It is ludicrous to suggest that the Government, if it is aware that an employee or former employee is about to disclose classified information, should not consider every lawful means to protect the nation's security. However, the possibility of infrequently seeking injunctive relief in no practical or even theoretical sense equates to mandatory prepublication review for every publication of every signer of the SF 189.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

ACTION

August 10, 1987

MEMORANDUM FOR GRANT S. GREEN, JR.

FROM:

BARRY KELLY *BK*

SUBJECT:

Classified Information Nondisclosure Agreement

Attached at Tab I is a draft response which was prepared by Steven Garfinkel (Tab II), from you to himself as Director, Information Security Oversight Office.

By letter dated June 24, 1987, Congressman Gerry Sikorski wrote Frank Carlucci expressing concern regarding implementation of NSDD 84 requiring all civil servants to sign a Classified Information Nondisclosure Agreement (SF 189), parts of which his committee found to contain "ambiguities and inconsistencies, as well as vague and questionable terms." A response was approved by Frank Carlucci (Tab III), clarifying the issues raised by Congressman Sikorski. We have learned that Sikorski has indicated his interest in holding joint hearings with Chairwoman Patricia Schroeder of the Subcommittee on Civil Service, who shared some of Sikorski's concerns about SF 189.

By letter (Tab IV) dated July 13, 1987, Chairwoman Schroeder makes clear that she is prepared to drop this matter if ISOO takes the regulatory steps, i.e., the submission of a directive to make non-substantive regulatory clarifications as were proposed in Steven Garfinkel's letter to her dated July 13, 1987, (Tab V) and suggested in their draft response to Congressman Sikorski.

Under these circumstances, Garfinkel believes that it is critical that we act promptly and affirmatively to help defuse this issue by making the non-substantive regulatory clarifications that we have proposed. He further believes that it would be beneficial if the recommendation to ISOO to proceed with these regulatory changes comes from the NSC. We agree with Garfinkel.

KS *SPK* *ABF*
Brenda Reger, Paul Stevens and Alison Fortier concur.

RECOMMENDATION

That you approve the draft response to Garfinkel at Tab I.

Approve *[Signature]*

Disapprove _____

Prepared by. *[Signature]* John F. Lewis

Attachments

Tab I Memo to Garfinkel
Tab II Incoming from Garfinkel
Tab III Carlucci's Letter to Sikorski
Tab IV Schroeder's Letter to Garfinkel
Tab V Garfinkel's Letter to Schroeder

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
03. Letter	For Mr Green From: Steven Garfinkel Re: Advisory Notice (3 pp.)	7/6/87	(b)(1)	C

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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

UNCLASSIFIED

Proposed Change to ISOO Directive No. 1

§ 2001.43 Storage

*

*

*

(a) Minimum requirements for physical barriers.

(1) Top Secret. Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type changeable combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret established under the provisions of § 2001.41. For Top Secret information stored outside the United States, one or more of the following supplementary controls is required:

(i) the area that houses the security container or vault shall be subject to the continuous protection of guard or duty personnel; (ii) guard or duty personnel shall inspect the security container or vault at least once every two hours; or (iii) the security container or vault shall be controlled by an alarm system to which a force will respond in person within 15 minutes. In addition, heads of agencies shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored.

UNCLASSIFIED

BARBARA BOXER
6TH DISTRICT, CALIFORNIA

COMMITTEE ON THE BUDGET

COMMITTEE ON ARMED SERVICES

SELECT COMMITTEE ON CHILDREN,
YOUTH, AND FAMILIES

WHIP AT LARGE



Congress of the United States
House of Representatives
Washington, DC 20515

4935
307 CANNON BUILDING
WASHINGTON, DC 20515
(202) 225-5181

DISTRICT OFFICES:
450 GOLDEN GATE AVENUE
SAN FRANCISCO, CA 94102
(415) 626-6943

88 BELVEDERE STREET
SAN RAFAEL, CA 94901
(415) 457-7272

421 STARR AVENUE
VALLEJO, CA 94590
(707) 552-0720

SONOMA
(707) 763-8033

June 23, 1987

Mr. Grant S. Green, Jr.
Executive Secretary
National Security Council
Washington, D.C. 20506

Dear Mr. Green:

I am requesting a copy of of National Security Decision Directive 197 and the cover memo that accompanied it. I understand the directive was signed in November, 1985 and part of it had to do with requiring federal employees to report any contacts with persons from the Soviet Union, Eastern Europe, Communist China and numerous other "countries of concern."

I would also like any documents that may have been issued by the National Security Council that may further explain and clarify the precise meaning and parameters of the directive. I am interested in this because I have received a letter from a union representing federal employees of the Treasury Department in my district, who are concerned that they will be held responsible for reporting all and any contacts, including contacts with relatives, with the public as part of their day to day business, and even contacts with employees of restaurants who are immigrants of those countries.

I look forward to your prompt reply.

Sincerely,

BARBARA BOXER
Member of Congress

BB:dm

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

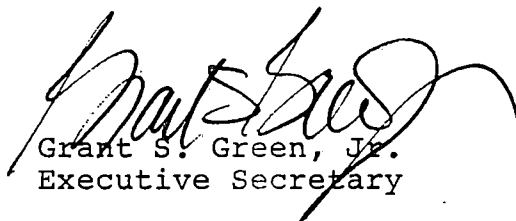
August 4, 1987

Dear Representative Boxer:

In response to your June 23, 1987 letter, I am forwarding to you a copy of National Security Decision Directive 197, entitled "Reporting Hostile Contacts and Security Awareness."

I note your concerns about the alleged possible impact on Treasury Department employees and would encourage you to contact the Department directly on that matter. I understand that Mr. Larry B. Sheafe, Director, Office of Security, Department of Treasury (Telephone 343-0260) is in a position to provide further details in this regard.

Sincerely,



Grant S. Green, Jr.
Executive Secretary

Attachments

cc: Executive Secretary,
Department of Treasury

The Honorable Barbara Boxer
House of Representatives
Washington, D.C. 20515

UNCLASSIFIED

November 1, 1985

REPORTING HOSTILE CONTACTS AND SECURITY AWARENESS

In addition to measures presently in place to provide for physical, information and personnel security against the hostile intelligence threat, the provisions of this directive will enhance overall government efforts to protect against illegal or unauthorized acquisition by hostile intelligence services of information and technology vital to our national interest.

Many agencies, particularly those directly involved in the United States intelligence effort, foreign affairs and military matters, have well-developed programs designed to maintain a high level of security awareness and to examine relationships of their employees with foreign nationals. Agencies whose primary mission requires that they maintain classified or otherwise sensitive information, while attractive targets for hostile foreign interests, are by no means the only agencies which are vulnerable to the loss of information or technology which may be critical to the ability of the United States to protect itself.

Responsibility for Security

Each department or agency of the US Government shall establish procedures which will:

- Create and maintain a formalized security awareness program designed to ensure a high level of awareness among its employees of the potential threat to its propriety, sensitive and classified information from foreign sources, whether overt or covert. This program must include a periodic formal briefing of the threat posed by hostile intelligence services.

- Provide for the reporting, under defined circumstances, of employee contacts with nationals of certain foreign countries or political entities as hereafter specified.

The nature and extent of this program will be commensurate with the potential for foreign interest in not only the classified information holdings of the department or agency, but also in its technological or other sensitive activities. The program should be tailored to meet the particular functions of the agency or department and the vulnerability of certain categories

Declassified/Released on 11/15/86
under provisions of E.O. 12356
by D. Reger, National Security Council

UNCLASSIFIED

Released
Full Text of
NSDD 197

of employees who, through either their job functions or access to classified or sensitive information or technology, invite targeting or exploitation by foreign intelligence services. The program should be designed so as not to intrude into the privacy of employees or into their freedom of association.

Reporting of Hostile Contacts

Each department or agency shall establish procedures which require its employees to report certain contacts.

- These procedures will require reporting of all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which:

-- Illegal or unauthorized access is sought to classified or otherwise sensitive information.

-- The employee is concerned that he or she may be the target of an attempted exploitation by a foreign entity.

- The procedures will also require reporting of any contacts with nationals of the Soviet Union and Soviet Bloc countries as well as other specific foreign countries or foreign political entities, which are determined by the department or agency in coordination with the Federal Bureau of Investigation as being of particular relevance to its security concerns. In implementing this procedure, the security officer or designated official of the department or agency will review and evaluate the reported information in accordance with the standards for reporting. The designation of particular countries as being of greater concern will provide a basis for the security officer or designated official to judge the relative importance of a particular contact. Any facts or circumstances of a reported contact with a hostile country which appear to (1) indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive and classified information, (2) which appear to offer a reasonable potential for such, or (3) indicate the possibility of continued professional or personal contacts, shall be reported promptly by the responsible department or agency to the FBI in the case of employees located in the United States and to the Central Intelligence Agency (CIA) in the case of employees located overseas. The CIA in turn will inform the FBI as appropriate.

Other Intelligence or Investigative Interests

Nothing in this directive is intended to modify the authority and responsibility of the Director of Central Intelligence or the Central Intelligence Agency for counterintelligence abroad, nor does it in any way change existing procedures or agreements between CIA and the Department of State and other U.S. agencies

UNCLASSIFIED

regarding the reporting of hostile contacts outside the U.S. Neither does it preclude interagency agreements or directives affecting the relationship between the FBI and other intelligence or investigative agencies regarding their responsibility for personnel, physical or document security or their territorial jurisdiction.

Review of Procedures

The head of each agency or department will provide a copy of its Security Awareness program and its procedures for reporting hostile contacts to the Assistant to the President for National Security Affairs for review by December 1, 1985.

UNCLASSIFIED

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

May 21, 1987

MEMORANDUM FOR NSC STAFF

FROM: GRANT S. GREEN JR. 

SUBJECT: Security Survey

In support of the National Security Advisor's goal of improving security within the NSC, the position of Director of Security Programs has been established under the Directorate of Information Policy and Security Review. The person selected to fill the position is Dorrance P. Howland who joined us last week.

The Director of Security will be conducting an in-depth security survey of the NSC. Our physical, personnel and technical security procedures will be examined, and where necessary, recommendations will be made, and corrective action implemented. Also, a system of documenting security procedures will be established.

Frank strongly supports the need for this action. We believe the NSC should not only provide our staff with the necessary guidance to establish a sense of confidence that our actions are consistent with good security, but should serve as a model for others within the national security community. I request your cooperation in these efforts to improve the security posture of the NSC.

NATIONAL SECURITY COUNCIL

April 25, 1985

MEMORANDUM FOR CHRISTOPHER HICKS

FROM: W. ROBERT PEARSON *WRP*
SUBJECT: Additional Information Reference the Installation
of Cipher Locks

Per a telephone conversation on April 16, 1985, the following information responds to your further questions concerning our memorandum of April 1.

Cost for Restoration of Doorways (Removal of Cipher Locks)

\$230 per doorway
\$5,980 for 26 doorways

Entrances where staffing could possibly ensure constant access control.*

Suite 351
Suite 365
Suite 368
Suite 392

* We are concerned that eliminating cipher locks from these four doorways is a risky way to proceed, but would be happy to work with you on any of these questions. We believe the Secret Service has made it clear that this type of access control would not be acceptable to them when PROFS is installed.

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
04. Memorandum	For Christopher Hicks From: Robert Kimmitt Re: Security (1 pp.)	4/1/85	(b)(1)	C

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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
05. Paper	Re: US Intelligence Community Physical Security Standards (10 pp.)	n.d.	(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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
06. Memorandum	For Edward Wilson From: Paul Thompson Re: Security Requirements (1 pp.)	11/1/84	(b)(1)	C

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 [3]

Date Closed: 9/4/2019

OA/ID Number: 99017-003

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]

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
07. Memorandum	For Security Officer From: Technical Security Division Re: Security Survey (3 pp.)	1/18/84	(b)(1)	C

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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

Optional (Continued)

() Government-Furnished Property (Short Form)	52.245-04
() Warranty of Supplies of a Noncomplex Nature	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate I	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate II	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate III	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate IV	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate V	52.246-17
() Warranty of Supplies of a Complex Nature	52.246-18
() Warranty of Supplies of a Complex Nature-Alternate I	52.246-18
() Warranty of Supplies of a Complex Nature-Alternate II	52.246-18
() Warranty of Supplies of a Complex Nature-Alternate III	52.246-18
() Warranty of Supplies of a Complex Nature-Alternate IV	52.246-18
() Warranty of Systems and Equipment under Performance Specifications or Design Criteria	52.246-19
() Warranty of Systems and Equipment under Performance Specifications or Design Criteria-Alternate I	52.246-19
() Warranty of Systems and Equipment under Performance Specifications or Design Criteria-Alternate II	52.246-19
() Warranty of Systems and Equipment under Performance Specifications or Design Criteria-Alternate III	52.246-19
() Limitation of Liability	52.246-33

(REMAINDER OF PAGE NOT USED.)

SECTION I - CONTRACT CLAUSES (CONTINUED)

() Report of Shipment (REPSHIP)	52.242-12
() Notification of Changes	52.243-07
() Subcontracts Under Fixed-Price Contracts	52.244-01
() Subcontracts Under Fixed-Price Contracts-Alternate I	52.244-01
() Competition in Subcontracting	52.244-05
() Property Records	52.245-01
() Government Property (Fixed-Price Contracts)	52.245-02
() Government Property (Fixed-Price Contracts)- Alternate I	52.245-02
() Use and Charges	52.245-09
() Special Tooling	52.245-17
() Special Tooling-Alternate I	52.245-17
() Special Test Equipment	52.245-18
() Government Property Furnished "As Is"	52.245-19
() Limitation of Liability	52.246-23
() Limitation of Liability-High-Value Items	52.246-24
() Limitation of Liability-High-Value Items-Alternate I	52.246-24
() Commercial Bill of Lading Notations	52.247-01
() Preference for U.S.-Flag Air Carriers	52.247-63
() Preference for Privately Owned U.S.-Flag Commercial Vessels	52.247-64
() Preference for Privately Owned U.S.-Flag Commercial Vessels-Alternate I	52.247-64
() Value Engineering	52.248-01
() Value Engineering-Alternate I	52.248-01
() Value Engineering-Alternate II	52.248-01
() Value Engineering-Alternate III	52.248-01
() Termination for Convenience of the Government (Fixed-Price) (Short-Term)	52.249-01
(X) Termination for Convenience of the Government (Fixed-Price)	52.249-02
() Termination for Convenience of the Government (Fixed-Price)-Alternate II	52.249-02
(X) Default (Fixed-Price Supply and Service)	52.249-08
() Indemnification Under Public Law 85-804	52.250-01
() Government Supply Sources	52.251-01
() Government Supply Sources-Alternate I	52.251-01

Optional

() Economic Price Adjustment-Labor and Material	52.216-04
() Incentive Subcontracting Program for Small and Disadvantaged Business Concerns	52.219-10
() Interest	52.232-17
() Change Order Accounting	52.243-06
[] Subcontracts Under Fixed-Price Contracts	52.244-01
[] Subcontracts Under Fixed-Price Contracts-Alternate I	52.244-01

SECTION I - CONTRACT CLAUSES (CONTINUED)

() Affirmative Action for Handicapped Workers-Alternate I	52.222-36
(X) Clean Air and Water	52.223-02
() Hazardous Material Identification and Material Safety Data	52.223-03
() Privacy Act Notification	52.224-01
() Privacy Act	52.224-02
() Buy American Act-Supplies	52.225-03
() Balance of Payments Program	52.225-07
() Buy American Act-Trade Agreements Act-Balance of Payments Program	52.225-09
() Duty-Free Entry	52.225-10
() Certain Communist Areas	52.225-11
() Bid Guarantee	52.228-01
() Additional Bond Security	52.228-02
() Insurance-Work on a Government Installation	52.228-05
(X) Federal, State, and Local Taxes	52.229-03
() Federal, State, and Local Taxes (Noncompetitive Contract)	52.229-04
() Taxes-Contracts Performed in U.S. Possessions or Puerto Rico	52.229-05
() Taxes-Foreign Fixed-Price Contracts	52.229-06
() Taxes-Fixed-Price Contracts with Foreign Governments	52.229-07
() Cost Accounting Standards	52.230-03
() Administration of Cost Accounting Standards	52.230-04
() Disclosure and Consistency of Cost Accounting Practices	52.230-05
() Consistency in Cost Accounting Practices	52.230-06
() Payments	52.232-01
() Discounts for Prompt Payment	52.232-08
() Limitation on Withholding of Payments	52.232-09
() Extras	52.232-11
() Progress Payments	52.232-16
() Progress Payments-Alternate I	52.232-16
() Interest	52.232-17
() Availability of Funds	52.232-18
() Assignment of Claims	52.232-23
() Assignment of Claims-Alternate I	52.232-23
() Prohibition of Assignment of Claims	52.232-24
(X) Disputes	52.233-01
() Disputes-Alternate I	52.233-01
(X) Protection of Government Buildings, Equipment, and Vegetation	52.237-02
() Notice of Intent to Disallow Costs	52.242-01
() Production Progress Reports	52.242-02
() F.o.b. Origin-Government Bills of Lading or Prepaid Postage	52.242-10
() F.o.b. Origin-Government Bills of Lading or Indicia Mail	52.242-11
() Advance Payments	52.232-12
() Advance Payments-Alternate I	52.232-12
() Advance Payments-Alternate III	52.232-12
() Advance Payments-Alternate IV	52.232-12

SECTION I - CONTRACT CLAUSES (CONTINUED)

() Subcontractor Cost or Pricing Data	52.215-24
() Subcontractor Cost or Pricing Data--Modifications	52.215-25
() Facilities Capital Cost of Money	52.215-30
() Waiver of Facilities Capital Cost of Money	52.215-31
() Price Redetermination--Prospective	52.216-05
() Price Redetermination--Retroactive	52.216-06
() Incentive Price Revision--Firm Target	52.216-16
() Incentive Price Revision--Firm Target--Alternate I	52.216-16
() Incentive Price Revision--Successive Targets	52.216-17
() Incentive Price Revision--Successive Targets-- Alternate I	52.216-17
() Execution and Commencement of Work	52.216-23
() Limitation of Government Liability	52.216-24
() Contract Definitization	52.216-25
() Contract Definitization--Alternate I	52.216-25
() Limitation of Price and Contractor Obligations	52.217-01
() Cancellation of Items	52.217-02
() Cancellation of Items--Alternate I	52.217-02
() Option for Increased Quantity	52.217-06
() Option for Increased Quantity--Separately Priced Line Item	52.217-07
() Notice of Total Small Business-Labor Surplus Area Set-Aside	52.219-05
() Notice of Total Small Business Set-Aside	52.219-06
() Notice of Partial Small Business Set-Aside	52.219-07
(X) Utilization of Small Business Concerns and Small Disadvantaged Business Concerns	52.219-08
() Small Business and Small Disadvantaged Business Subcontracting Plan	52.219-09
() Small Business and Small Disadvantaged Business Subcontracting Plan--Alternate I	52.219-09
(X) Utilization of Women-Owned Small Businesses	52.219-13
(X) Preference for Labor Surplus Area Concerns	52.220-01
() Notice of Total Labor Surplus Area Set-Aside	52.220-02
(X) Utilization of Labor Surplus Area Concerns	52.220-03
() Labor Surplus Area Subcontracting Program	52.220-04
() Notice to the Government of Labor Disputes	52.222-01
(X) Convict Labor	52.222-03
() Contract Work Hours and Safety Standards--Overtime Compensation--General	52.222-04
() Contract Work Hours and Safety Standards--Overtime Compensation--Firefighters and Fireguards	52.222-05
() Walsh-Healey Public Contracts Act	52.222-20
(X) Equal Opportunity	52.222-26
() Equal Opportunity--Alternate I	52.222-26
() Equal Opportunity Preaward Clearance of Subcontracts	52.222-28
() Notification of Visa Denial	52.222-29
(X) Affirmative Action for Special Disabled and Vietnam Era Veterans	52.222-35
() Affirmative Action for Special Disabled and Vietnam Era Veterans--Alternate I	52.222-35
(X) Affirmative Action for Handicapped Workers	52.222-36

SECTION I - CONTRACT CLAUSES

I-1 CONTRACT CLAUSES FOR FIXED-PRICE SUPPLY CONTRACTS

The following contract clauses (indicated by an "X" in the left hand column) are hereby incorporated by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

<u>Title</u>	<u>FAR Citation*</u>
(X) Definitions	52.202-01
(X) Covenant Against Contingent Fees	52.203-05
(X) Changes--Fixed-Price	52.243-01
(x) Officials Not to Benefit	52.203-01
(X) Gratuities	52.203-03
() Approval of Contract	52.204-01
() Security Requirements	52.204-02
() Right of First Refusal of Employment	52.207-03
() Required Sources for Jewel Bearings and Related Items	52.208-01
() First Article Approval-Contractor Testing	52.209-03
() First Article Approval-Contractor Testing-Alternate I	52.209-03
() First Article Approval-Contractor Testing-Alternate II	52.209-03
() First Article Approval-Government Testing	52.209-04
() First Article Approval-Government Testing-Alternate I	52.209-04
() First Article Approval-Government Testing-Alternate II	52.209-04
() New Material	52.210-05
() Used or Reconditioned Material, Residual Inventory, and Former Government Surplus Property	52.210-07
() Priorities, Allocations, and Allotments	52.212-08
() Fast Payment Procedure	52.213-01
() Audit-Formal Advertising	52.214-26
() Price Reduction for Defective Cost or Pricing Data-Modifications-Formal Advertising	52.214-27
() Subcontractor Cost or Pricing Data-Modifications-Formal Advertising	52.214-28
() Examination of Records by Comptroller General	52.215-01
() Audit-Negotiation	52.215-02
() Changes or Additions to Make-or-Buy Program	52.215-21
() Changes or Additions to Make-or-Buy Program-Alternate I	52.215-21
() Changes or Additions to Make-or-Buy Program-Alternate II	52.215-21
() Price Reduction for Defective Cost or Pricing Data	52.215-22
() Price Reduction for Defective Cost or Pricing Data-Modifications	52.215-23

*"FAR Citation" refers to the Federal Acquisition Regulation (48 CFR-Chapter 1).

SECTION H - SPECIAL CONTRACT REQUIREMENTS

CONTRACT ORDER OF PRECEDENCE

In the event of an inconsistency between the provisions of this contract, the inconsistency shall be resolved by giving precedence in the following order: (a) the Schedule (excluding the Specifications); (b) Terms and Conditions of the Solicitation, if any; (c) General Provisions; (d) other provisions of the contract, when attached or incorporated by reference; (e) the Specifications; and (f) such portions of the Contractor's Technical Proposal as may be incorporated into the contract.

(REMAINDER OF PAGE NOT USED.)

SECTION G - CONTRACT ADMINISTRATION DATA (CONTINUED)

Executive Office of the President
National Security Council
17th and Pennsylvania Avenue, N.W.
Rm. 397, OEOB
Washington, D.C. 20500

ATTN: Mary Dix
Phone: (202) 395- 6868

Each invoice must include:

- A. Contract number
- B. Description of product or service provided
- C. Serial Numbers of Machines (if applicable)
- D. Unit Prices of each item
- E. Total amount of invoice
- F. Payment terms
- G. Name, title, phone number and complete mailing address of responsible official to whom payment is to be sent.

(REMAINDER OF PAGE NOT USED)

SECTION G - CONTRACT ADMINISTRATION (CONTINUED)

No new work assignments, which would require the employment of additional personnel, or which would increase or decrease the estimated costs or period of performance, or affect any provision of this contract, may be made without approval of the Contracting Officer. Program and work modifications will, however, be expected as essential to the conduct of an effective information management program, responsible to changing needs of management and staff in a dynamic work environment. Such modifications will be accommodated by adjustments in existing programs, mutually agreed upon by the Contracting Officer's Technical Representative (COTR) and the Contractor. Work to be performed under this contract shall be subject to the technical direction of the COTR.

If, in the opinion of the contractor, any instruction or direction issued by the COTR is not provided for in any of the clauses of the contract, the contractor shall not proceed but shall notify the Contracting Officer in writing within five (5) working days after the receipt of any such instruction or direction and shall request the Contracting Officer to modify the contract accordingly. Upon receiving such notification from the contractor, the Contracting Officer shall issue an appropriate contract modification or advise the contractor in writing that, in his/her opinion, the technical direction is within the scope of this clause and does not constitute a change under the Changes Clause of the contract. The contractor shall thereupon proceed immediately with the direction given.

A failure of the parties to agree upon the nature of the instruction or direction or upon the contract action to be taken with respect thereto shall be subject to the provision of the contract clause entitled "Disputes."

G.4 PAYMENT

In return for satisfactory performance and compliance with the terms and conditions of this contract, the Government will pay the Contractor upon submission by the Contractor of an invoice in an original and two copies. Invoices should be sent to the following address for certification prior to payment:

SECTION G - CONTRACT ADMINISTRATION DATA (CONTINUED)

(4) performing technical inspections and acceptances required by this contract; and (5) assisting the Contractor in the resolution of technical problems encountered during performance. The Contracting Officer is responsible for directing or negotiating any changes in the terms, conditions, or amounts cited in the contract.

- d. For guidance from the COTR to the Contractor to be valid, it must: (1) be consistent with the description of the work set forth in the contract; (2) not constitute new assignments of work or change to the expressed terms, conditions, or specifications incorporated into this contract; (3) not constitute a basis for an extension to the period of performance or contract delivery schedule; (4) not constitute a basis for any increase in the contract cost.
- e. On all matters that pertain to the contract terms the Contractor must communicate with the Contracting Officer. Whenever, in the opinion of the Contractor, the COTR requests effort outside the scope of this contract, the Contractor should so advise the COTR. If the COTR persists and there still exists a disagreement as to the proper contractual coverage, the Contracting Officer should be notified immediately, preferably in writing if time permits. Proceeding with work without proper contractual coverage could result in non-payment or necessitate the submittal of costly claims under the contract.
- f. The COTR may be changed by the Government at any time without prior notice to the Contractor. Written notice to the Contractor will be given by the Contracting Officer to effect any change in COTR(s).

G.3. TECHNICAL DIRECTION

Technical Direction, as used herein, will be the overseeing of the Contractor and its staff to insure compliance with all of the items in the contract. It will include elaboration of the Specifications (Section C) by filling in details or otherwise completing the general description of work set forth by the contract schedule.

SECTION G - CONTRACT ADMINISTRATION

G.1 CONTRACTUAL INFORMATION

Contractual interpretation and assistance may be obtained by contacting:

Executive Office of the President
Office of Administration
Procurement and Contracts
Room 498, OEOB
17th and Pennsylvania Avenue, N.W.
Washington, D.C. 20500

ATTN: Nancy Roth
Phone: (202) 395-3314

G.2 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE

- a. The Contracting Officer hereby designates the below named individual as the COTR:

Name: Mary Dix

Address: Executive Office of the President
National Security Council
17th and Pennsylvania Avenue, N.W.
Room 397, OEOB
Washington, D.C. 20500

Phone: (202) 395-6868

- b. The COTR is responsible for administering the performance of work under this contract. In no event, however, will any understanding, agreement, modification, change order, or other matter deviating from the terms of this contract be effective or binding upon the Government unless formalized by proper contractual documents executed by the Contracting Officer prior to completion of the contract.
- c. The COTR is responsible for: (1) monitoring the Contractor's technical progress, including the surveillance and assessment of performance and recommending to the Contracting Officer changes in requirements; (2) interpreting the scope of work; (3) performing technical evaluation as required;

SECTION B - SUPPLIES SERVICES AND PRICES

The Contractor shall install a permissive entry device on 26 main entrances of National Security Offices

Codetronics model 1999 with key override
(26 each at \$2,700.00 each) TOTAL COST \$70,200.00

Remote access capability and associated
electrical requirements
(26 each at \$300.00 each) TOTAL \$7,800.00

TOTAL COST - \$78,000.00

SECTION C - SPECIFICATIONS

(NOT APPLICABLE)

SECTION D - PACKAGING AND MARKING

(NOT APPLICABLE)

SECTION E - INSPECTION AND ACCEPTANCE

This section incorporates the following contract clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

<u>TITLE</u>	<u>FAR CITATION*</u>
Inspection of Supplies - Fixed Price	52.246-02
Inspection of Services - Fixed Price	52.246-04

*FAR Citation refers to the Federal Acquisition Regulation (48 CFR, Chapter 1)

SECTION F - DELIVERIES AND PERFORMANCE

The Contractor shall deliver and install the entry devices within eight (8) months after contract award at the installations indicated by Mary Dix of the National Security Council.

STANDARD FORM 26 (REV. 10-81)
Prescribed by GSA

SOLE SOURCE JUSTIFICATION AND RECOMMENDATION

Suburban Contractors, Inc. is an eminently well qualified firm to undertake this project. They have done extensive work in this area and have the necessary cleared personnel to accomplish the task in this controlled security environment. Moreover, the nature of the work is of such a sensitive nature that disclosing plans and concepts to the general public is not in the best interest of National security. Recommend no other contractor be brought into competition for this project and Suburban Contractors, Inc. be given the task on an expeditious basis.

~~CONFIDENTIAL~~

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

September 26, 1984

MEMORANDUM FOR JOHN P. BRADY
DIRECTOR, ADMINISTRATIVE OPERATIONS DIVISION
OFFICE OF ADMINISTRATION

FROM: MARY A. DIX *Mary A. Dix*
SUBJECT: Waiver of Notification in the Commerce
Business Daily

In addition to being required for security purposes, the need for the procurement and installation of permissive entry devices by the National Security Council is of such urgency that the interests of the Government would be adversely affected if the time requirement for advance notice were complied with.

Hence, having determined that advance notice is neither appropriate nor reasonable, publication of the intended procurement action in the Commerce Business Daily should be waived pursuant with sections (e) (1) (A), (B), and (H) of Public Law 98-72.

~~CONFIDENTIAL~~
Declassify on: OADR

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

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
08. Memorandum	For John Brady From: Mary Dix Re: Justification of Sole Source Procurement (1 pp.)	9/26/84	(b)(1)	C

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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
09. Form	Procurement File Copy (1 pp.)	9/26/84	(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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

NATIONAL SECURITY COUNCIL

October 5, 1984

MEMORANDUM FOR JOHN F. W. ROGERS
ASSISTANT TO THE PRESIDENT FOR
MANAGEMENT AND ADMINISTRATION

FROM: ROBERT M. KIMMITT *Bob*
SUBJECT: Installation of Permissive Entry Devices

The U.S. Secret Service has recently completed a survey of NSC offices and has provided recommendations that ensure full compliance with standards set forth in National Security Council and Director of Central Intelligence Directives pertaining to the safeguarding of Sensitive Compartmented Intelligence. On their instructions we are required to install a permissive entry device on the entrances of the NSC offices.

As we are aware of the historical significance of the Old Executive Office Building, we would appreciate the coordination of this effort with your office.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20508

October 30, 1984

MEMORANDUM FOR JOHN P. BRADY
DIRECTOR, ADMINISTRATIVE OPERATIONS DIVISION,
OFFICE OF ADMINISTRATION *

FROM: MARY A. DIX *Mary A. Dix*
ADMINISTRATIVE OFFICER

SUBJECT: Installation of Permissive Entry Devices

As per your request, the following is a list of the 26 doorways
requiring cipher locks (permissive entry devices):

300	302	348
351	361	361½
365	368	372
373	374	374-A
375	376-A	376
380	382	386
389	391	392
395	397	477
479	487	

Also, accompanying this memorandum is the actual device that will
be installed inside the doorways. Wherever possible, the entry
devices will be installed in the same manner as the one on Room
81/DEOB. By following this installation procedure, the overall
physical view of the corridors will not be effected unless one
faces an individual doorway and examines the inner wall.

Please notify me when you have completed your review of the
attached permissive entry device.

Thank you.

Optional (Continued)

() Government-Furnished Property (Short Form)	52.245-04
() Warranty of Supplies of a Noncomplex Nature	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate I	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate II	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate III	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate IV	52.246-17
() Warranty of Supplies of a Noncomplex Nature-Alternate V	52.246-17
() Warranty of Supplies of a Complex Nature	52.246-18
() Warranty of Supplies of a Complex Nature-Alternate I	52.246-18
() Warranty of Supplies of a Complex Nature-Alternate II	52.246-18
() Warranty of Supplies of a Complex Nature-Alternate III	52.246-18
() Warranty of Supplies of a Complex Nature-Alternate IV	52.246-18
() Warranty of Systems and Equipment under Performance Specifications or Design Criteria	52.246-19
() Warranty of Systems and Equipment under Performance Specifications or Design Criteria-Alternate I	52.246-19
() Warranty of Systems and Equipment under Performance Specifications or Design Criteria-Alternate II	52.246-19
() Warranty of Systems and Equipment under Performance Specifications or Design Criteria-Alternate III	52.246-19
() Limitation of Liability	52.246-33

(REMAINDER OF PAGE NOT USED.)

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
10. Memorandum	For Paul Thompson Re: Status of Security Upgrade (2 pp.)	3/7/85	(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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

CONFIDENTIAL

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

~~CONFIDENTIAL~~

DECLASSIFIED

PER NSC WAIVER, 1500 2021-02
By SS NARA, Date 9/13/24

March 27, 1987

C.F.

2115

506326

F0008-03

CO165

FE

FH011

FH00612

MEMORANDUM FOR DISTRIBUTION LIST

ACWA, et al

SUBJECT:

Promulgation of Policy re Visa Applications for
Personnel Assigned to the USSR (U)

OBJECTIVE: To establish a means of regulating and monitoring all Soviet visa applications made by U.S. Government personnel who are being sent on permanent assignment to U.S. diplomatic missions in the USSR (Moscow and Leningrad). (C)

HISTORY/SETTING: Currently, all agencies independently submit visa applications for their personnel to the Soviet Embassy. The USSR has imposed a personnel ceiling on our diplomatic missions on the basis of the number of Soviet visas which have been issued for permanent staff as opposed to presence in country. These measures taken by the Soviet Union on October 22, 1986, which limit the number of employees permitted at the American Embassy in Moscow to 225 and at our Consulate General in Leningrad to 26, require the following action. (C)

POLICY: To ensure that visas are issued in a timely fashion and are issued to those individuals most needed by our missions in the USSR and to verify the number of visas issued by the Soviets -- visa submissions must be regulated by a central authority. The Department of State will serve as the central point for regulating Soviet visa applications and will coordinate applications under the ceiling to ensure that basic U.S. Government objectives are met. This procedure will have no impact on each agency's procedures for selecting persons for assignment to Moscow or Leningrad. It would not go into effect until an individual who has been assigned to a permanent position in Moscow or Leningrad reaches the point when he should apply for a Soviet visa. (C)

ACTIONS/IMPLEMENTATION: All Executive Branch agencies should henceforth process requests for Soviet visas for their personnel through the Office of Soviet Union Affairs of the Department of State. Passports, completed Soviet visa application forms and

~~CONFIDENTIAL~~

Declassify: OADR

C O P Y
from ORM

CONFIDENTIAL

NSC#8702115

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

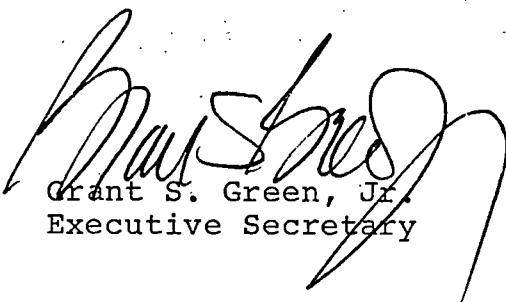
2

one picture (which is essential for the visa application) for all personnel and their dependents should be sent to EUR/SOV, Room 4225 (telephone: 647-8956 or 647-0670). (Ø)

The Department of State will coordinate submissions with Embassy Moscow and will submit the visa applications for U.S. personnel assigned to permanent positions to the Soviet Embassy in Washington. The passport and visa application should be accompanied by the name and telephone number of a contact person for use by EUR/SOV, should any questions arise. (Ø)

Individuals already assigned outside the United States and who do not intend to return to the U.S. before departing for assignment in the USSR should, by message, seek authority from EUR/SOV to apply for a Soviet visa from Soviet posts abroad. Upon receipt of State Department authorization, those individuals may apply for a visa directly to a Soviet post convenient to them. No application will be submitted to a Soviet post prior to receipt of a message authorizing such application. (Ø)

Should disagreements which cannot otherwise be resolved arise between Executive Branch agencies and the Department of State pursuant to this Directive, they should be referred to the Office of Soviet and European Affairs, National Security Council for review. (U)


Grant S. Green, Jr.
Executive Secretary

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

MEMORANDUM

NATIONAL SECURITY COUNCIL

1002

ACTION

~~CONFIDENTIAL~~

UNCLASSIFIED WHEN SEPARATED
FROM CLASSIFIED ATTACHMENT

March 12, 1985

MEMORANDUM FOR ROBERT KIMMITT

THRU: BOB PEARSON *WBP* **SIGNED**
FROM: MARY DIX *Mary*
SUBJECT: Cipher Locks

Attached for your review and signature is a memorandum to Christopher Hicks requesting approval of installation of cipher locks outside NSC offices.

RECOMMENDATION

That you sign the attached memorandum/packet for forwarding to the Office of Administration.

APPROVE

K

DISAPPROVE

Attachment
Memo to OA

~~CONFIDENTIAL~~

UNCLASSIFIED WHEN SEPARATED
FROM CLASSIFIED ATTACHMENT

DECLASSIFIED
White House Guidelines
E.O. 13526, SEC 3.4 (b), September 11, 2006
By MB NARA, Date 9/4/19

~~CONFIDENTIAL~~

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
12. Memorandum	For Robert McFarlane From: Paula Dobriansky Re: Imposition of Travel Restrictions (2 pp.)	12/10/85	(b)(1)	S

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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
13. Memorandum	For Robert McFarlane From: Nicholas Platt Re: Imposition of Travel Restrictions (1 pp.)	12/2/85	(b)(1)	S

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 [3]

Date Closed: 9/4/2019

OA/ID Number: 99017-003

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]

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
14. Paper	Re: NSDD 196 - Counterintelligence/Countermeasure Implementation Task Force (5 pp.)	11/1/85	(b)(1)	S

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 [3]

Date Closed: 9/4/2019	OA/ID Number: 99017-003
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]

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

January 18, 1984

Dear Senator Wilson:

Thank you for your inquiry concerning National Security Decision Directive (NSDD) 84 and related initiatives to safeguard national security information.

Executive Order 12356 on "National Security Information" defines the types of information that may and may not be classified and limits the authority to make such determinations to authorized classifiers. Once that determination is made, all Federal employees who have chosen to work in positions involving national security information have the responsibility to protect properly classified information. The President reminded employees of this obligation in a letter dated August 30, 1983, which refers to the directive (NSDD 84) on safeguarding national security information.

We have received numerous requests for information on this subject, and our staff has put together the attached information package.

It is hoped that the enclosed materials will provide the basis for a better understanding of the purposes of NSDD 84 and related initiatives to safeguard national security information.

Sincerely,



Brenda S. Reger
Director
Office of Information Policy
and Security Review

Attachments

The Honorable Pete Wilson
11000 Wilshire Blvd., Suite 11221
Los Angeles, CA 90024
Attention: Mr. Don Ediger

March 11, 1983

Safeguarding National Security Information

As stated in Executive Order 12356, only that information whose disclosure would harm the national security interests of the United States may be classified. Every effort should be made to declassify information that no longer requires protection in the interest of national security.

At the same time, however, safeguarding against unlawful disclosures of properly classified information is a matter of grave concern and high priority for this Administration. In addition to the requirements set forth in Executive Order 12356, and based on the recommendations contained in the interdepartmental report forwarded by the Attorney General, I direct the following:

1. Each agency of the Executive Branch that originates or handles classified information shall adopt internal procedures to safeguard against unlawful disclosures of classified information. Such procedures shall at a minimum provide as follows:

a. All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access. This requirement may be implemented prospectively by agencies for which the administrative burden of compliance would otherwise be excessive.

b. All persons with authorized access to Sensitive Compartmented Information (SCI) shall be required to sign a nondisclosure agreement as a condition of access to SCI and other classified information. All such agreements must include a provision for prepublication review to assure deletion of SCI and other classified information.

c. All agreements required in paragraphs 1.a. and 1.b. must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States. The Director, Information Security Oversight Office (ISOO), shall develop standardized forms that satisfy these requirements.

d. Appropriate policies shall be adopted to govern contacts between media representatives and agency personnel, so as to reduce the opportunity for negligent or deliberate disclosures of classified information. All persons with authorized access to classified information shall be clearly apprised of the agency's policies in this regard.

UNCLASSIFIED

Full Text of

2. Each agency of the Executive branch that originates or handles classified information shall adopt internal procedures to govern the reporting and investigation of unauthorized disclosures of such information. Such procedures shall at a minimum provide that:

a. All such disclosures that the agency considers to be seriously damaging to its mission and responsibilities shall be evaluated to ascertain the nature of the information disclosed and the extent to which it had been disseminated.

b. The agency shall conduct a preliminary internal investigation prior to or concurrently with seeking investigative assistance from other agencies.

c. The agency shall maintain records of disclosures so evaluated and investigated.

d. Agencies in the possession of classified information originating with another agency shall cooperate with the originating agency by conducting internal investigations of the unauthorized disclosure of such information.

e. Persons determined by the agency to have knowingly made such disclosures or to have refused cooperation with investigations of such unauthorized disclosures will be denied further access to classified information and subjected to other administrative sanctions as appropriate.

3. Unauthorized disclosures of classified information shall be reported to the Department of Justice and the Information Security Oversight Office, as required by statute and Executive orders. The Department of Justice shall continue to review reported unauthorized disclosures of classified information to determine whether FBI investigation is warranted. Interested departments and agencies shall be consulted in developing criteria for evaluating such matters and in determining which cases should receive investigative priority. The FBI is authorized to investigate such matters as constitute potential violations of federal criminal law, even though administrative sanctions may be sought instead of criminal prosecution.

4. Nothing in this directive is intended to modify or preclude interagency agreements between FBI and other criminal investigative agencies regarding their responsibility for conducting investigations within their own agencies or departments.

5. The Office of Personnel Management and all departments and agencies with employees having access to classified information are directed to revise existing regulations and policies, as necessary, so that employees may be required to submit to polygraph examinations, when appropriate, in the course of investigations of unauthorized disclosures of classified information. As a minimum, such regulations shall permit an agency to decide that appropriate

UNCLASSIFIED

adverse consequences will follow an employee's refusal to cooperate with a polygraph examination that is limited in scope to the circumstances of the unauthorized disclosure under investigation. Agency regulations may provide that only the head of the agency, or his delegate, is empowered to order an employee to submit to a polygraph examination. Results of polygraph examinations should not be relied upon to the exclusion of other information obtained during investigations.

6. The Attorney General, in consultation with the Director, Office of Personnel Management, is requested to establish an interdepartmental group to study the federal personnel security program and recommend appropriate revisions in existing Executive orders, regulations, and guidelines.

11/11/2011

Embargoed for Conclusion of Background Briefing
Held March 11, 1983, at the Department of Justice

Fact Sheet

Presidential Directive on
Safeguarding National Security Information

Background

- Unlawful disclosures of classified information damage national security by providing valuable information to our adversaries, by hampering the ability of our intelligence agencies to function effectively, and by impairing the conduct of American foreign policy.
- The President has issued a directive requiring that additional steps be taken to protect against unlawful disclosures of classified information.
- This directive is based on the recommendations of an inter-departmental group convened by the Attorney General.

Scope of Directive

- The directive deals only with disclosures of classified information.
- By Executive Order, the only information that can be classified is information which "reasonably could be expected to cause damage to the national security" if released without proper authorization. (E.O. 12356 § 1.1(a)(3).)
- The Executive Order also prohibits the use of classification to conceal violations of law, inefficiency or administrative error, or to prevent an embarrassment to a government agency or employee. (E.O. 12356 § 1.6(a).)

Summary of Provisions

- The directive imposes additional restrictions upon government employees who are entrusted with access to classified information, and upon government agencies that originate or handle classified information.
- More employees will be required to sign nondisclosure agreements, including provisions for prepublication review, such as were approved by the Supreme Court in United States v. Snepp (1980).

Agencies will be required to adopt policies concerning contacts between journalists and persons with access to classified information, so as to reduce opportunities for unlawful disclosures. However, no particular policies are mandated in the directive.

- Agencies will be required to adopt new procedures so that unlawful disclosures of classified information will be reported and analyzed more efficiently.
- The directive establishes a new approach to investigating unlawful disclosures to replace the past practice of treating such matters as purely criminal investigations.
 - Although unauthorized disclosures of classified information potentially violate a number of criminal statutes, there has never been a successful prosecution. There are a number of practical barriers to successful criminal prosecution in most of these cases.
 - This directive clarifies FBI's authority to investigate unlawful disclosures of classified information, even though it is anticipated that a successful investigation will lead to administrative sanctions (such as demotion or dismissal) rather than criminal prosecution.
 - All agencies with employees having access to classified information will be required to assure that their policies permit use of polygraph examinations under carefully defined circumstances. The polygraph is already used on a regular basis by our largest intelligence agencies. The directive provides for a greater degree of consistency in government-wide policy regarding use of this investigative technique.
 - The use of the polygraph in any particular case will be subject to the discretion of an employee's agency head.
 - There will be no change in the current practice of targeting investigations at employees who are suspected of unlawfully disclosing classified information, rather than at journalists who publish it.

- The directive provides that employees found by their agency head to have knowingly disclosed classified information without authorization or to have refused cooperation with investigations will be subject to mandatory administrative sanctions to include, as a minimum, denial of further access to classified information. Existing procedural safeguards for personnel actions involving federal employees remain unchanged.

Expected Results

- This directive is not expected to eliminate all unlawful disclosures of classified information.
- The directive is designed to improve the effectiveness of our present program and, over time, to reduce the frequency and seriousness of unlawful disclosures of classified information.
- The directive also emphasizes that government employees who are entrusted with classified information have a fiduciary duty to safeguard that information from unauthorized disclosure.

THE WHITE HOUSE

WASHINGTON

August 30, 1983

MEMORANDUM FOR FEDERAL EMPLOYEES

SUBJECT: Unauthorized Disclosure of Classified Information

Recent unauthorized disclosures of classified information concerning our diplomatic, military, and intelligence activities threaten our ability to carry out national security policy. I have issued a directive detailing procedures to curb these disclosures and to streamline procedures for investigating them. However, unauthorized disclosures are so harmful to our national security that I wish to underscore to each of you the seriousness with which I view them.

The unauthorized disclosure of our Nation's classified information by those entrusted with its protection is improper, unethical, and plain wrong. This kind of unauthorized disclosure is more than a so-called "leak"--it is illegal. The Attorney General has been asked to investigate a number of recent disclosures of classified information. Let me make it clear that we intend to take appropriate administrative action against any Federal employee found to have engaged in unauthorized disclosure of classified information, regardless of rank or position. Where circumstances warrant, cases will also be referred for criminal prosecution.

The American people have placed a special trust and confidence in each of us to protect their property with which we are entrusted, including classified information. They expect us to protect fully the national security secrets used to protect them in a dangerous and difficult world. All of us have taken an oath faithfully to discharge our duties as public servants, an oath that is violated when unauthorized disclosures of classified information are made.

Secrecy in national security matters is a necessity in this world. Each of us, as we carry out our individual duties, recognizes that certain matters require confidentiality. We must be able to carry out diplomacy with friends and foes on a confidential basis; peace often quite literally depends on it--and this includes our efforts to reduce the threat of nuclear war.

We must also be able to protect our military forces from present or potential adversaries. From the time of the Founding Fathers, we have accepted the need to protect military secrets. Nuclear dangers, terrorism, and aggression similarly demand

that we must be able to gather intelligence information about these dangers--and our sources of this information must be protected if we are to continue to receive it. Even in peacetime, lives depend on our ability to keep certain matters secret.

As public servants, we have no legitimate excuse for resorting to these unauthorized disclosures. There are other means available to express ourselves:

- We make every effort to keep the Congress and the people informed about national security policies and actions. Only a fraction of information concerning national security policy must be classified.
- We have mechanisms for presenting alternative views and opinions within our government.
- Established procedures exist for declassifying material and for downgrading information that may be overclassified.
- Workable procedures also exist for reporting wrongdoing or illegalities, both to the appropriate Executive Branch offices and to the Congress.

Finally, each of us has the right to leave our position of trust and criticize our government and its policies, if that is what our conscience dictates. What we do not have is the right to damage our country by giving away its necessary secrets.

We are as a Nation an open and trusting people, with a proud tradition of free speech, robust debate, and the right to disagree strongly over all national policies. No one would ever want to change that. But we are also a mature and disciplined people who understand the need for responsible action. As servants of the people, we in the Federal Government must understand the duty we have to those who place their trust in us. I ask each of you to join me in redoubling our efforts to protect that trust.

Ronald Reagan

Tuesday
April 6, 1982

Part IV

The President

**Executive Order 12356—
National Security Information**

Presidential Documents

Page 3—

Executive Order 12356 of April 2, 1982

The President

National Security Information

TABLE OF CONTENTS

	/FR Page/
Preamble	[14874]
<i>Part 1. Original Classification</i>	
1.1 Classification Levels	[14874]
1.2 Classification Authority	[14874]
1.3 Classification Categories	[14875]
1.4 Duration of Classification	[14876]
1.5 Identification and Markings	[14877]
1.6 Limitations on Classification	[14877]
<i>Part 2. Derivative Classification</i>	
2.1 Use of Derivative Classification	[14878]
2.2 Classification Guides	[14878]
<i>Part 3. Declassification and Downgrading</i>	
3.1 Declassification Authority	[14878]
3.2 Transferred Information	[14879]
3.3 Systematic Review for Declassification	[14879]
3.4 Mandatory Review for Declassification	[14879]
<i>Part 4. Safeguarding</i>	
4.1 General Restrictions on Access	[14880]
4.2 Special Access Programs	[14881]
4.3 Access by Historical Researchers and Former Presidential Appointees	[14881]
<i>Part 5. Implementation and Review</i>	
5.1 Policy Direction	[14881]
5.2 Information Security Oversight Office	[14881]
5.3 General Responsibilities	[14882]
5.4 Sanctions	[14882]
<i>Part 6. General Provisions</i>	
6.1 Definitions	[14883]
6.2 General	[14883]

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

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

Part 1

Original Classification

Section 1.1 *Classification Levels.*

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

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

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

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

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

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

Sec. 1.2 Classification Authority.

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

- (1) the President;
- (2) agency heads and officials designated by the President in the Federal Register; and
- (3) officials delegated this authority pursuant to Section 1.2(d).

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

- (1) agency heads and officials designated by the President in the Federal Register;
- (2) officials with original Top Secret classification authority; and
- (3) officials delegated such authority pursuant to Section 1.2(d).

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

- (1) agency heads and officials designated by the President in the Federal Register;
- (2) officials with original Top Secret or Secret classification authority; and
- (3) officials delegated such authority pursuant to Section 1.2(d).

(d) Delegation of Original Classification Authority.

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

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

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

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification author-

ity; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original classification authority by the agency head.

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

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

Sec. 1.3 *Classification Categories.*

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

- (1) military plans, weapons, or operations;
- (2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
- (3) foreign government information;
- (4) intelligence activities (including special activities), or intelligence sources or methods;
- (5) foreign relations or foreign activities of the United States;
- (6) scientific, technological, or economic matters relating to the national security;
- (7) United States Government programs for safeguarding nuclear materials or facilities;
- (8) cryptology;
- (9) a confidential source; or
- (10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

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

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

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

Sec. 1.4 Duration of Classification.

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

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

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

Sec. 1.5 Identification and Markings.

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

- (1) one of the three classification levels defined in Section 1.1;
- (2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;
- (3) the agency and office of origin; and
- (4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

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

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

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

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

Sec. 1.6 Limitations on Classification.

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

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

(c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information

may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1), or an official with original Top Secret classification authority.

Part 2

Derivative Classification

Sec. 2.1 Use of Derivative Classification.

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

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

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

Sec. 2.2 Classification Guides.

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

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

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

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

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

Part 3

Declassification and Downgrading

Sec. 3.1 Declassification Authority.

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

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).

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

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

Sec. 3.2 Transferred Information.

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

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

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

Sec. 3.3 Systematic Review for Declassification.

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

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

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

Sec. 3.4. Mandatory Review for Declassification.

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

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

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

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

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

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

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

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

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

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

Part 4

Safeguarding

Sec. 4.1 General Restrictions on Access.

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

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

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

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

Sec. 4.2 Special Access Programs.

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

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

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

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

- (1) are engaged in historical research projects, or
- (2) previously have occupied policy-making positions to which they were appointed by the President.

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

- (1) determines in writing that access is consistent with the interest of national security;
- (2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and
- (3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

Implementation and Review

Sec. 5.1 Policy Direction.

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

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

Sec. 5.2 Information Security Oversight Office.

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

(b) The Director shall:

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

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

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

(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

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

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

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

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

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

Sec. 5.3 General Responsibilities.

Agencies that originate or handle classified information shall:

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

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

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

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

Sec. 5.4 Sanctions.

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official

designated under Section 5.3(a)(1) so that corrective steps, if appropriate, may be taken.

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

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

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

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

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

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

Part 6

General Provisions

Sec. 6.1 Definitions.

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

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

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

(d) "Foreign government information" means:

(1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

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

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

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

Sec. 6.2 General.

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

declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

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

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

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

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

Ronald Reagan

THE WHITE HOUSE,
April 2, 1982.

[FR Doc. 82-9320

Filed 4-2-82; 2:52 pm]

Billing code 3195-01-M

Editorial Note: The President's statement of Apr. 2, 1982, on signing Executive Order 12356 is printed in the *Weekly Compilation of Presidential Documents* (vol. 18, no. 13)

Federal Register

Vol. 47, No. 70

Monday, April 12, 1982

Presidential Documents

Title 3—

Executive Order 12356 of April 2, 1982

The President

National Security Information

Correction

In the April 6, 1982 issue of the Federal Register, there appear on pages 14875, 14876, 14878, 14882 and 14883 incorrect references to "Section 5.3(a)(1)" of Executive Order 12356 of April 2, 1982. All references on these pages to "Section 5.3(a)(1)" should read "Section 5.3(a)."

Richard A. Hauser
Deputy Counsel to the President
April 8, 1982.

[FR Doc. 82-10124

Filed 4-9-82; 9:11 am]

Billing code 3195-01-M



would you like to know

if any changes have been made in certain titles of the **CODE OF FEDERAL REGULATIONS** without reading the **Federal Register** every day? If so, you may wish to subscribe to the **LSA (List of CFR Sections Affected)**, the "**Federal Register Index**," or both.

LSA (List of CFR Sections Affected)
\$10.00
per year

The **LSA (List of CFR Sections Affected)** is designed to lead users of the **Code of Federal Regulations** to amendatory actions published in the **Federal Register**, and is issued monthly in cumulative form. Entries indicate the nature of the changes.

Federal Register Index **\$8.00**
per year

Indexes covering the contents of the daily **Federal Register** are issued monthly in cumulative form. Entries are carried primarily under the names of the issuing agencies. Significant subjects are carried as cross-references.

A finding aid is included in each publication which lists **Federal Register** page numbers with the date of publication in the **Federal Register**.

Note to **FR** Subscribers: **FR** Indexes and the **LSA (List of CFR Sections Affected)** will continue to be mailed free of charge to regular **FR** subscribers.

Mail order form to:
Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402

There is enclosed \$_____ for _____ subscription(s) to the publications checked below:

_____ **LSA (LIST OF CFR SECTIONS AFFECTED)** (\$10.00 a year domestic; \$12.50 foreign)

_____ **FEDERAL REGISTER INDEX** (\$8.00 a year domestic; \$10.00 foreign)

Name _____

Street Address _____

City _____ State _____ ZIP _____

Make check payable to the Superintendent of Documents

Friday
June 25, 1982

Part VIII

Information Security
Oversight Office

National Security Information

INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2001

Directive No. 1]

National Security Information

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Implementing Directive; final rule.

SUMMARY: The Information Security Oversight Office is publishing this Directive (final rule) pursuant to section 5.2(b)(1) of Executive Order 12356, relating to national security information. The National Security Council approved this Directive on June 22, 1982. The Executive order prescribes a uniform information security system; it also establishes a monitoring system to enhance its effectiveness. This Directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of national security information.

EFFECTIVE DATE: August 1, 1982.

FOR FURTHER INFORMATION CONTACT:

Steven Garfinkel, Director, ISOO.
Telephone: 202-535-7251.

SUPPLEMENTARY INFORMATION: This Directive is issued pursuant to the provisions of section 5.2(b)(1) of Executive Order 12356. The purpose of the Directive is to assist in implementing the Order; users of the Directive shall refer concurrently to that Order for guidance.

List of Subjects in 32 CFR Part 2001

Archives and records, Authority delegations, Classified information, Executive orders, Freedom of information, Information, Intelligence, National defense, National security information, Presidential documents, Security information, Security measures.

Title 32 of the Code of Federal Regulations, Part 2001, is revised to read as follows:

PART 2001—NATIONAL SECURITY INFORMATION

Subpart A—Original Classification

- Sec.
- 2001.1 Classification levels.
 - 2001.2 Classification authority.
 - 2001.3 Classification categories.
 - 2001.4 Duration of classification.
 - 2001.5 Identification and markings.
 - 2001.6 Limitations on classification.

Subpart B—Derivative Classification

- 2001.20 Use of derivative classification.
- 2001.21 Classification guides.

- Sec.
- 2001.22 Derivative identification and markings.

Subpart C—Declassification and Downgrading

- 2001.30 Listing declassification and downgrading authorities.
- 2001.31 Systematic review for declassification.
- 2001.32 Mandatory review for declassification.
- 2001.33 Assistance to the Department of State.
- 2001.34 FOIA and Privacy Act requests.

Subpart D—Safeguarding

- 2001.40 General.
- 2001.41 Standards for security equipment.
- 2001.42 Accountability.
- 2001.43 Storage.
- 2001.44 Transmittal.
- 2001.45 Special access programs.
- 2001.46 Reproduction controls.
- 2001.47 Loss or possible compromise.
- 2001.48 Disposition and destruction.
- 2001.49 Responsibilities of holders.
- 2001.50 Emergency planning.
- 2001.51 Emergency authority.

Subpart E—Implementation and Review

- 2001.60 Agency regulations.
- 2001.61 Security education.
- 2001.62 Oversight.

Subpart F—General Provisions

- 2001.70 Definitions.
- 2001.71 Publication and effective date.

Authority: Section 5.2(b)(1), E.O. 12356. 47 FR 14874, April 8, 1982.

Subpart A—Original Classification

§ 2001.1 Classification levels.

(a) *Limitations [1.1(b)].* Markings other than "Top Secret," "Secret," and "Confidential," such as "For Official Use Only" or "Limited Official Use," shall not be used to identify national security information. No other term or phrase shall be used in conjunction with these markings, such as "Secret Sensitive" or "Agency Confidential," to identify national security information. The terms "Top Secret," "Secret," and "Confidential" should not be used to identify nonclassified executive branch information.

(b) *Reasonable doubt [1.1(c)].* (1) When there is reasonable doubt about the need to classify information, the information shall be safeguarded as if it were "Confidential" information in accordance with Subpart D, pending the determination about its classification. Upon the determination of a need for classification, the information that is classified shall be marked as provided in § 2001.5.

(2) When there is reasonable doubt about the appropriate classification

¹ Bracketed references pertain to related sections of Executive Order 12356.

level, the information shall be safeguarded at the higher level in accordance with Subpart D, pending the determination about its classification level. Upon the determination of its classification level, the information shall be marked as provided in § 2001.5.

§ 2001.2 Classification authority.

(a) *Requests for original classification authority [1.2 and 5.2(b)(5)].* A request for original classification authority pursuant to section 1.2 of Executive Order 12356 (hereinafter "the Order") shall include a complete justification for the level of classification authority sought, a description of the information that will require original classification, and the anticipated frequency of original classification actions.

(b) *Listing classification authorities [1.2].* Agencies shall maintain a current listing of officials delegated original classification authority by name, position, or other identifier. If possible, this listing shall be unclassified.

(c) *Exceptional cases [1.2(e)].* Information described in section 1.2(e) of the Order shall be protected as provided in § 2001.1(b).

§ 2001.3 Classification categories.

(a) *Classification in context of related information [1.3(b)].* Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

(b) *Unofficial publication or disclosure [1.3(d)].* Following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with the Order or predecessor orders, the agency of primary interest shall determine the degree of damage to the national security, the need for continued classification, and, in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences.

§ 2001.4 Duration of classification.

(a) *Information not marked for declassification [1.4].* Information classified under predecessor orders that is not subject to automatic declassification shall remain classified until reviewed for declassification.

(b) *Authority to extend automatic declassification determinations [1.4(b)].* The authority to extend the

classification of information subject to automatic declassification under predecessor orders is limited to those officials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Director of the Information Security Oversight Office.

§ 2001.5 Identification and markings
[1.5(a), 1.5(b) and 1.5(c)].

A uniform information security system requires that standard markings be applied to national security information. Except in extraordinary circumstances as provided in section 1.5(a) of the Order, or as indicated herein, the marking of paper documents created after the effective date of the Order shall not deviate from the following prescribed formats. These markings shall also be affixed to material other than paper documents, or the originator shall provide holders or recipients of the information with written instructions for protecting the information.

(a) *Classification level.* The markings "Top Secret," "Secret," and "Confidential" are used to indicate: that information requires protection as national security information under the Order; the highest level of classification contained in a document; and the classification level of each page and, in abbreviated form, each portion of a document.

(1) *Overall marking.* The highest level of classification of information in a document shall be marked in such a way as to distinguish it clearly from the informational text. These markings shall appear at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

(2) *Page marking.* Each interior page of a classified document shall be marked at the top and bottom either according to the highest classification of the content of the page, including the designation "Unclassified" when it is applicable, or with the highest overall classification of the document.

(3) *Portion marking.* Agency heads may waive the portion marking requirement for specified classes of documents or information only upon a written determination that: (i) There will be minimal circulation of the specified documents or information and minimal potential usage of these documents or information as a source for derivative classification determinations; or (ii) there is some other basis to conclude

that the potential benefits of portion marking are clearly outweighed by the increased administrative burdens. Unless the portion marking requirement has been waived as authorized, each portion of a document, including subjects and titles, shall be marked by placing a parenthetical designation immediately preceding or following the text to which it applies. The symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used for this purpose. If the application of parenthetical designations is not practicable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification, and the information that is not classified. If all portions of a document are classified at the same level, this fact may be indicated by a statement to that effect. If a subject or title requires classification, an unclassified identifier may be applied to facilitate reference.

(b) *Classification authority.* If the original classifier is other than the signer or approver of the document, the identity shall be shown as follows:

"CLASSIFIED BY (identification of original classification authority)"

(c) *Agency and office of origin.* If the identity of the originating agency and office is not apparent on the face of a document, it shall be placed below the "CLASSIFIED BY" line.

(d) *Declassification and downgrading instructions.* Declassification and, as applicable, downgrading instructions shall be shown as follows:

(1) For information to be declassified automatically on a specific date:

"DECLASSIFY ON: (date)"

(2) For information to be declassified automatically upon occurrence of a specific event:

"DECLASSIFY ON: (description of event)"

(3) For information not to be declassified automatically:

"DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED or 'OADR'"

(4) For information to be downgraded automatically on a specific date or upon occurrence of a specific event:

"DOWNGRADE TO (classification level) ON (date or description of event)"

(e) *Special markings.*—(1) *Transmittal documents [1.5(c)].* A transmittal document shall indicate on its face the highest classification of any information transmitted by it. It shall also include the following or similar instruction:

(i) For an unclassified transmittal document:

"UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS REMOVED"

(ii) For a classified transmittal document:

"UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS (classification level of the transmittal document standing alone)"

(2) *"Restricted Data" and "Formerly Restricted Data" [6.2(a)].* "Restricted Data" and "Formerly Restricted Data" shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended.

(3) *Intelligence sources or methods [1.5(c)].* Documents that contain information relating to intelligence sources or methods shall include the following marking unless otherwise proscribed by the Director of Central Intelligence:

"WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED"

(4) *Foreign government information [1.5(c)].* Documents that contain foreign government information shall include either the marking "FOREIGN GOVERNMENT INFORMATION," or a marking that otherwise indicates that the information is foreign government information. If the fact that information is foreign government information must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin.

(5) *Computer output [1.5(c)].* Documents that are generated as computer output may be marked automatically by systems software. If automatic marking is not practicable, such documents must be marked manually.

(6) *Agency prescribed markings [1.5(c), 4.2(a), and 5.3(c)].* Officials delegated original classification authority by the President may prescribe additional markings to control reproduction and dissemination, including markings required for special access programs authorized by section 4.2(a) of the Order.

(f) *Electrically transmitted information (messages) [1.5(c)].* National security information that is transmitted electrically shall be marked as follows:

(1) The highest level of classification shall appear before the first line of text;

(2) A "CLASSIFIED BY" line is not required;

(3) The duration of classification shall appear as follows:

(i) For information to be declassified automatically on a specific date:

"DECL: (date)"

(ii) For information to be declassified upon occurrence of a specific event:

"DECL: (description of event)"

(iii) For information not to be automatically declassified which requires the originating agency's determination (see also § 2001.5(d)(3)):

"DECL: OADR"

(iv) For information to be automatically downgraded:

"DNG (abbreviation of classification level to which the information is to be downgraded and date or description of event on which downgrading is to occur)"

(4) Portion marking shall be as prescribed in § 2001.5(a)(3);

(5) Special markings as prescribed in § 2001.5(e) (2), (3), and (4) shall appear after the marking for the highest level of classification. These include:

(i) "Restricted Data" and "Formerly Restricted Data" shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended;

(ii) Information concerning intelligence sources or methods: "WNINTEL," unless proscribed by the Director of Central Intelligence;

(iii) Foreign government information: "FGL" or a marking that otherwise indicates that the information is foreign government information. If the fact that information is foreign government information must be concealed, the marking shall not be used and the message shall be marked as if it were wholly of U.S. origin.

(6) Paper copies of electrically transmitted messages shall be marked as provided in § 2001.5(a) (1) and (2).

(g) *Changes in classification markings* [1.4(b) and 4.1(b)]. When a change is made in the duration of classified information, all holders of record shall be promptly notified. If practicable, holders of record shall also be notified of a change in the level of classification. Holders shall alter the markings to conform to the change, citing the authority for it. If the remarking of large quantities of information is unduly burdensome, the holder may attach a change of classification notice to the storage unit in lieu of the marking action otherwise required. Items withdrawn from the collection for purposes other than transfer for storage shall be marked promptly in accordance with the change notice.

§ 2001.6 Limitations on classification [1.6(c)].

Before reclassifying information as provided in section 1.6(c) of the Order, the authorized official shall consider the following factors, which shall be

addressed in the report to the Director of the Information Security Oversight Office:

(a) The elapsed time following disclosure;

(b) The nature and extent of disclosure;

(c) The ability to bring the fact of reclassification to the attention of persons to whom the information was disclosed;

(d) The ability to prevent further disclosure; and

(e) The ability to retrieve the information voluntarily from persons not authorized access in its reclassified state.

Subpart B—Derivative Classification

§ 2001.20 Use of derivative classification [2.1].

The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized original classifier or in accordance with an authorized classification guide. If a person who applies derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult for a determination an appropriate official of the originating agency or office of origin who has the authority to upgrade, downgrade, or declassify the information.

§ 2001.21 Classification guides.

(a) *General* [2.2(a)]. Classification guides shall, at a minimum:

(1) Identify or categorize the elements of information to be protected;

(2) State which classification level applies to each element or category of information; and

(3) Prescribe declassification instructions for each element or category of information in terms of (i) a period of time, (ii) the occurrence of an event, or (iii) a notation that the information shall not be declassified automatically without the approval of the originating agency.

(b) *Requirement for review* [2.2(a)]. Classification guides shall be reviewed at least every two years and updated as necessary. Each agency shall maintain a list of its classification guides in current use.

(c) *Waivers* [2.2(c)]. An authorized official's decision to waive the requirement to issue classification

guides for specific classes of documents or information should be based, at a minimum, on an evaluation of the following factors:

(1) The ability to segregate and describe the elements of information;

(2) The practicality of producing or disseminating the guide because of the nature of the information;

(3) The anticipated usage of the guide as a basis for derivative classification; and

(4) The availability of alternative sources for derivatively classifying the information in a uniform manner.

§ 2001.22 Derivative identification and markings [1.5(c) and 2.1(b)].

Documents classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2001.5(a) through (e) as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide.

(a) *Classification authority*. The authority for classification shall be shown as follows:

"CLASSIFIED BY (description of source document or classification guide)"

If a document is classified on the basis of more than one source document or classification guide, the authority for classification shall be shown as follows:

"CLASSIFIED BY MULTIPLE SOURCES"

In these cases the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. A document derivatively classified on the basis of a source document that is marked "CLASSIFIED BY MULTIPLE SOURCES" shall cite the source document in its "CLASSIFIED BY" line rather than the term "MULTIPLE SOURCES."

(b) *Declassification and downgrading instructions*. Dates or events for automatic declassification or downgrading, or the notation "ORIGINATING AGENCY'S DETERMINATION REQUIRED" to indicate that the document is not to be declassified automatically, shall be carried forward from the source document, or as directed by a classification guide, and shown on a "DECLASSIFY ON" line as follows:

"DECLASSIFY ON: (date; description of event; or 'ORIGINATING AGENCY'S DETERMINATION REQUIRED' (OADR))"

Subpart C—Declassification and Downgrading

§ 2001.30 Listing declassification and downgrading authorities [3.1(b)].

Agencies shall maintain a current listing of officials delegated declassification or downgrading authority by name, position, or other identifier. If possible, this listing shall be unclassified.

§ 2001.31 Systematic review for declassification [3.3].

(a) *Permanent records.* Systematic review is applicable only to those classified records and presidential papers or records that the Archivist of the United States, acting under the Federal Records Act, has determined to be of sufficient historical or other value to warrant permanent retention.

(b) *Non-permanent records.* Non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services under the Records Disposal Act. These schedules shall provide for the continued retention of records subject to an ongoing mandatory review for declassification request.

(c) *Responsibilities.* (1) In meeting responsibilities assigned by section 3.3(a) of the Order, the Archivist shall:

(i) Establish procedures, in consultation with the Director of the Information Security Oversight Office, for the systematic declassification review of permanent classified records accessioned into the National Archives and classified presidential papers or records under the Archivist's control;

(ii) Conduct systematic declassification reviews in accordance with guidelines provided by the head of the agency that originated the information; or, with respect to foreign government information, in accordance with guidelines provided by the head of the agency having declassification jurisdiction over the information, or, if no guidelines have been provided, in accordance with the general guidelines provided by the Director of the Information Security Oversight Office after coordination with the agencies having declassification authority over the information; or, with respect to presidential papers or records, in accordance with guidelines developed by the Archivist and approved by the National Security Council;

(iii) Conduct systematic declassification reviews of accessioned records and presidential papers or records as they become 30 years old, except for file series concerning intelligence activities (including special

activities), or intelligence sources or methods created after 1945, and information concerning cryptology created after 1945;

(iv) Conduct systematic declassification reviews of accessioned records and presidential papers or records in file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945 and cryptology records created after 1945 as they become fifty years old;

(v) Establish systematic review priorities for accessioned records and presidential papers or records based on the degree of researcher interest and the potential for declassifying a significant portion of the information;

(vi) Re-review for declassification accessioned records and presidential papers or records upon the determination that the followup review will be productive, both in terms of researcher interest and the potential for declassifying a significant portion of the information.

(2) The Archivist may review for declassification, with the concurrence of the originating agency, accessioned records and presidential papers or records, prior to the timeframes established in paragraphs (c)(1) (iii) and (iv) of this section.

(3) Officials delegated original classification authority by the President under the Order or predecessor orders shall:

(i) Within six months of the effective date of the Order issue guidelines for systematic declassification review and, if applicable, for downgrading. These guidelines shall be developed in consultation with the Archivist and the Director of the Information Security Oversight Office and be designed to assist the Archivist in the conduct of systematic reviews;

(ii) Designate experienced personnel to provide timely assistance to the Archivist in the systematic review process;

(iii) Review and update guidelines for systematic declassification review and downgrading at least every five years unless earlier review is requested by the Archivist.

(4) Within six months of the effective date of the Order the Director of the Information Security Oversight Office shall issue, in consultation with the Archivist and the agencies having declassification authority over the information, general guidelines for the systematic declassification review of foreign government information. Also within six months, agency heads may issue, in consultation with the Archivist and the Director of the Information

Security Oversight Office, specific systematic declassification review guidelines for foreign government information over which the agency head has declassification authority. These guidelines shall be reviewed and updated every five years unless earlier review is requested by the Archivist.

(d) *Special procedures.* All agency heads shall be bound by the special procedures for systematic review of classified cryptologic records and classified records pertaining to intelligence activities (including special activities), or intelligence sources or methods issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

§ 2001.32 Mandatory review for declassification [3.4].

(a) *U.S. originated information.* (1) Each agency head shall publish in the Federal Register the identity of the person(s) or office(s) to which mandatory declassification review requests may be addressed.

(2) *Processing.* (i) *Requests for classified records in the custody of the originating agency.* A valid mandatory declassification review request need not identify the requested information by date or title of the responsive records, but must be of sufficient particularity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Agency responses to mandatory declassification review requests shall be governed by the amount of search and review time required to process the request. In responding to mandatory declassification review requests, agencies shall either make a prompt declassification determination and notify the requester accordingly, or inform the requester of the additional time needed to process the request. Agencies shall make a final determination within one year from the date of receipt except in unusual circumstances. When information cannot be declassified in its entirety, agencies will make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon the denial of an initial request, the agency shall also notify the requester of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial.

(ii) *Requests for classified records in the custody of an agency other than the originating agency.* When an agency receives a mandatory declassification review request for records in its

possession that were originated by another agency, it shall forward the request to that agency. The forwarding agency shall include a copy of the records requested together with its recommendations for action. Upon receipt, the originating agency shall process the request in accordance with § 2001.32(a)(2)(i). Upon request, the originating agency shall communicate its declassification determination to the referring agency.

(iii) *Appeals of denials of mandatory declassification review requests.* The agency appellate authority shall normally make a determination within 30 working days following the receipt of an appeal. If additional time is required to make a determination, the agency appellate authority shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The agency appellate authority shall notify the requester in writing of the final determination and of the reasons for any denial.

(b) *Foreign government information.* Except as provided in this paragraph, agency heads shall process mandatory declassification review requests for classified records containing foreign government information in accordance with § 2001.32(a). The agency that initially received or classified the foreign government information shall be responsible for making a declassification determination after consultation with concerned agencies. If the agency receiving the request is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request.

(c) *Cryptologic and intelligence information.* Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

(d) *Fees.* In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with section 483a of title 31, United States Code. The schedules of fees published in the Federal Register by agencies in implementation of Executive Order 11652 shall remain in effect until they are revised.

§ 2001.33 Assistance to the Department of State [3.3(b)].

Heads of agencies should assist the Department of State in its preparation of the *Foreign Relations of the United States* (FRUS) series by facilitating access to appropriate classified material in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

§ 2001.34 FOIA and Privacy Act requests [3.4].

Agency heads shall process requests for declassification that are submitted under the provisions of the Freedom of Information Act, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

Subpart D—Safeguarding

§ 2001.40 General [4.1].

Information classified pursuant to this Order or predecessor orders shall be afforded a level of protection against unauthorized disclosure commensurate with its level of classification. For information in special access programs established under the provisions of section 4.2 of the Order, the safeguarding requirements of Subpart D may be modified by the agency head responsible for creating the special access program as long as the modified requirements provide appropriate protection for the information.

§ 2001.41 Standards for security equipment [4.1(b) and 5.1(b)].

The Administrator of General Services shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for security equipment designed to provide secure storage for and to destroy classified information. Any agency may establish more stringent standards for its own use. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type available through the Federal Supply System.

§ 2001.42 Accountability [4.1(b)].

(a) *Top Secret.* Top Secret control officials shall be designated to receive, transmit, and maintain current access and accountability records for Top Secret information. An inventory of Top Secret documents shall be made at least annually. Agency heads may waive the requirement for an annual inventory of storage systems containing large volumes of Top Secret information upon a determination that the safeguarding of

this information is not jeopardized by the inventory waiver. Waivers shall be in writing and be available for review by the Information Security Oversight Office.

(b) *Secret and Confidential.* Agency heads shall prescribe accountability or control requirements for Secret and Confidential information.

§ 2001.43 Storage [4.1(b)].

Classified information shall be stored only in facilities or under conditions designed to prevent unauthorized persons from gaining access to it.

(a) *Minimum requirements for physical barriers.* (1) *Top Secret.* Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type changeable combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret established under the provisions of § 2001.41. In addition, heads of agencies shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored.

(2) *Secret and Confidential.* Secret and Confidential information shall be stored in a manner and under the conditions prescribed for Top Secret information, or in a container, vault, or alarmed area that meets the standards for Secret or Confidential information established under the provisions of § 2001.41. Secret and Confidential information may also be stored in a safe-type filing cabinet having a built-in, three-position, dial-type changeable combination lock, or a steel filing cabinet equipped with a steel lock bar secured by a GSA-approved three-position changeable combination padlock. Heads of agencies shall prescribe supplementary controls for storage of Secret information in cabinets equipped with a steel lock bar. Access to bulky Secret and Confidential material in weapons storage areas, strong rooms, closed areas or similar facilities shall be controlled in accordance with requirements established by the appropriate agency head. At a minimum, such requirements shall prescribe the use of key-operated, high-security padlocks approved by the General Services Administration.

(b) *Combinations.* (1) *Equipment in service.* Combinations to dial-type locks shall be changed only by persons having an appropriate security clearance, and shall be changed whenever such equipment is placed in use; whenever a person knowing the combination no

longer requires access to it; whenever a combination has been subjected to possible compromise; whenever the equipment is taken out of service; or at least once every year. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information that is protected by the lock.

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

(c) *Keys.* Heads of agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock.

§ 2001.44 Transmittal [4.1(b)].

(a) *Preparation and receipting.* Classified information to be transmitted outside of a facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, the addressee, and the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Any of these wrapping and receipting requirements may be waived by agency heads if conditions provide at least equivalent protection to prevent access by unauthorized persons.

(b) *Transmittal of Top Secret.* The transmittal of Top Secret information outside of a facility shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system authorized for the purpose, or over authorized secure communications circuits.

(c) *Transmittal of Secret.* The transmittal of Secret information shall be effected in the following manner:

(1) *The 50 States, the District of Columbia, and Puerto Rico.* Secret

information may be transmitted within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico by one of the means authorized for Top Secret information, by the U.S. Postal Service registered mail, or by protective services provided by U.S. air or surface commercial carriers under such conditions as may be prescribed by the head of the agency concerned.

(2) *Other areas.* Secret information may be transmitted from, to, or within areas other than those specified in § 2001.44(c)(1) by one of the means established for Top Secret information, or by U.S. registered mail through Military Postal Service facilities provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard U.S. Government and U.S. Government contract vehicles or aircraft, ships of the United States Navy, civil service manned U.S. Naval ships, and ships of U.S. registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are U.S. citizens and who are appropriately cleared may be designated as escorts.

(d) *Transmittal of Confidential.* Confidential information shall be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions by one of the means established for higher classifications, or by the U.S. Postal Service certified, first class, or express mail service when prescribed by an agency head. Outside these areas, Confidential information shall be transmitted only as is authorized for higher classifications.

(e) *Hand carrying of classified information.* Agency regulations shall prescribe procedures and appropriate restrictions concerning the escort or hand carrying of classified information, including the hand carrying of classified information on commercial carriers.

§ 2001.45 Special access programs [1.2(a) and 4.2(a)].

Agency heads designated pursuant to section 1.2(a) of the Order may create or continue a special access program if:

- (a) Normal management and safeguarding procedures do not limit access sufficiently; and
- (b) the number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information.

§ 2001.46 Reproduction controls [4.1(b)].

(a) Top Secret documents, except for the controlled initial distribution of information processed or received electrically, shall not be reproduced without the consent of the originator.

(b) Unless restricted by the originating agency, Secret and Confidential documents may be reproduced to the extent required by operational needs.

(c) Reproduced copies of classified documents shall be subject to the same accountability and controls as the original documents.

(d) Paragraphs (a) and (b) of this section shall not restrict the reproduction of documents to facilitate review for declassification.

§ 2001.47 Loss or possible compromise [4.1(b)].

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated for this purpose by the person's agency or organization. The agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The agency under whose cognizance the loss or possible compromise occurred shall initiate an inquiry to (a) determine cause, (b) place responsibility, and (c) take corrective measures and appropriate administrative, disciplinary, or legal action.

§ 2001.48 Disposition and destruction [4.1(b)].

Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of chapters 21 and 33 of title 44, United States Code, which govern disposition of Federal records. Classified information approved for destruction shall be destroyed in accordance with procedures and methods prescribed by the head of the agency. The method of destruction must preclude recognition or reconstruction of the classified information or material.

§ 2001.49 Responsibilities of holders [4.1(b)].

Any person having access to and possession of classified information is responsible for: (a) Protecting it from persons not authorized access to it, to include securing it in approved equipment or facilities whenever it is not under the direct supervision of

authorized persons; and (b) meeting accountability requirements prescribed by the head of the agency.

§ 2001.50 Emergency planning [4.1(b)].
Agencies shall develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. These plans shall include the disposition of classified information located in foreign countries.

§ 2001.51 Emergency authority [4.1(b)].
Those officials delegated original classification authority by the President may prescribe by regulation special provisions for the dissemination, transmittal, destruction, and safeguarding of national security information during combat or other emergency situations which pose an imminent threat to national security information.

Subpart E—Implementation and Review

§ 2001.60 Agency regulations [5.3(b)].
Each head of an agency shall issue regulations in accordance with 5 U.S.C. 552(a) to implement the Order and 32 CFR Part 2001 no later than December 31, 1982. Those portions that affect members of the public shall include, at a minimum, information relating to the agency's mandatory declassification review program and instructions for submitting suggestions or complaints regarding the agency's information security program.

§ 2001.61 Security education [5.3(a)].
Each agency that creates or handles national security information is required under the Order to establish a security

education program. The program established shall be sufficient to familiarize all necessary personnel with the provisions of the Order and its implementing directives and regulations and to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

§ 2001.62 Oversight [5.3(a)].

Agency heads shall require that periodic formal reviews be made to ensure compliance with the provisions of the Order and ISOO directives.

Subpart F—General Provisions

§ 2001.70 Definitions [6.1].

(a) *Original classification authority.* The authority vested in an executive branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(b) *Classification guide.* A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified on a derivative basis.

(c) *Originating agency.* The agency responsible for the initial determination that particular information is classified.

(d) *Multiple sources.* The term used to indicate that a document is derivatively classified when it contains classified information derived from more than one source.

(e) *Portion.* A segment of a document for purposes of expressing a unified theme; ordinarily a paragraph.

(f) *Special access program.* Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but is not limited to, special clearance, adjudication, or investigative requirements, special designations of officials authorized to determine "need-to-know," or special lists of persons determined to have a "need-to-know."

(g) *Intelligence activity.* An activity that an agency within the Intelligence Community is authorized to conduct pursuant to Executive Order 12333.

(h) *Special activity.* An activity conducted in support of national foreign policy objectives abroad which is planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activity, but which is not intended to influence United States political processes, public opinion, policies, or media and does not include diplomatic activities or the collection and production of intelligence or related support functions.

(i) *Unauthorized disclosure.* A communication or physical transfer of classified information to an unauthorized recipient.

§ 2001.71 Publication and effective date [6.2(e)].

Part 2001 shall be published in the Federal Register. It shall become effective August 1, 1982.

Steven Garfinkel,
Director, Information Security Oversight
Office.

June 23, 1982.

[FR Doc. 82-17235 Filed 6-23-82; 10:37 am]

BILLING CODE 6820-AF-M



Washington, D.C. 20530

August 25, 1983

Materials Concerning Prepublication Review

- 1) SCI Nondisclosure Agreement Form
- 2) Classified Information Nondisclosure Agreement Form
- 3) DOJ Letters on Enforceability of Agreements
- 4) DOJ Implementing Regulations

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name-Printed or Typed)

1 1. Intending to be legally bound, I hereby accept the obligations
2 contained in this Agreement in consideration of my being granted
3 access to information known as Sensitive Compartmented Information
4 (SCI). I have been advised and am aware that SCI involves or
5 derives from intelligence sources or methods and is classified or
6 classifiable under the standards of Executive Order 12356 or under
7 other Executive order or statute. I understand and accept that by
8 being granted access to SCI, special confidence and trust shall be
9 placed in me by the United States Government.

1 2. I hereby acknowledge that I have received a security indoctrination
2 concerning the nature and protection of SCI, including the procedures
3 to be followed in ascertaining whether other persons to whom I
4 contemplate disclosing this information have been approved for
5 access to it, and that I understand these procedures. I understand that
6 I may be required to sign subsequent agreements as a condition of
7 being granted access to different categories of SCI. I further
8 understand that all my obligations under this Agreement continue to
9 exist whether or not I am required to sign such subsequent agreements.

1 3. I have been advised and am aware that direct or indirect unauthorized
2 disclosure, unauthorized retention, or negligent handling of SCI by
3 me could cause irreparable injury to the United States or could be
4 used to advantage by a foreign nation. I hereby agree that I will
5 never divulge such information unless I have officially verified
6 that the recipient has been properly authorized by the United States
7 Government to receive it or I have been given prior written notice of
8 authorization from the United States Government Department or Agency
9 (hereinafter Department or Agency) last granting me either a security
10 clearance or an SCI access approval that such disclosure is permitted.

1 4. I further understand that I am obligated to comply with laws and
2 regulations that prohibit the unauthorized disclosure of classified
3 information. As used in this Agreement, classified information is
4 information that is classified under the standards of E.O. 12356, or
5 under any other Executive order or statute that prohibits the
6 unauthorized disclosure of information in the interest of national
7 security.

1 5. In consideration of being granted access to SCI and of being
2 assigned or retained in a position of special confidence and trust
3 requiring access to SCI and other classified information, I hereby
4 agree to submit for security review by the Department or Agency
5 last granting me either a security clearance or an SCI access
6 approval all materials, including works of fiction, that I contemplate
7 disclosing to any person not authorized to have such information,

8 or that I have prepared for public disclosure, which contain or
9 purport to contain:

- 10 (a) any SCI, any description of activities that produce or
- 11 relate to SCI, or any information derived from SCI;
- 12 (b) any classified information from intelligence reports
- 13 or estimates; or
- 14 (c) any information concerning intelligence activities,
- 15 sources or methods.

16 I understand and agree that my obligation to submit such information
17 and materials for review applies during the course of my access to
18 SCI and at all times thereafter. However, I am not required to
19 submit for review any such materials that exclusively contain
20 information lawfully obtained by me at a time when I have no employment,
21 contract or other relationship with the United States Government,
22 and which are to be published at such time.

1 6. I agree to make the submissions described in paragraph 5 prior
2 to discussing the information or materials with, or showing them to
3 anyone who is not authorized to have access to such information. I
4 further agree that I will not disclose such information or materials
5 unless I have officially verified that the recipient has been
6 properly authorized by the United States Government to receive it or
7 I have been given written authorization from the Department or
8 Agency last granting me either a security clearance or an SCI
9 access approval that such disclosure is permitted.

1 7. I understand that the purpose of the review described in paragraph 5
2 is to give the United States a reasonable opportunity to determine
3 whether the information or materials submitted pursuant to paragraph 5
4 set forth any SCI or other information that is subject to classification
5 under E.O. 12356 or under any other Executive order or statute that
6 prohibits the unauthorized disclosure of information in the interest
7 of national security. I further understand that the Department or
8 Agency to which I have submitted materials will act upon them,
9 coordinating with the Intelligence Community or other agencies when
10 appropriate, and substantively respond to me within 30 working days
11 from date of receipt.

1 8. I have been advised and am aware that any breach of this Agreement
2 may result in the termination of any security clearances and SCI
3 access approvals that I may hold; removal from any position of
4 special confidence and trust requiring such clearances or access
5 approvals; and the termination of my employment or other relationships
6 with the Departments or Agencies that granted my security clearances
7 or SCI access approvals. In addition, I have been advised and am
8 aware that any unauthorized disclosure of SCI or other classified
9 information by me may constitute a violation or violations of United
10 States criminal laws, including the provisions of Sections 641, 793,
11 794, 798, and 952, Title 18, United States Code, the provisions

12 of Section 783(b), Title 50, United States Code, and the provisions
13 of the Intelligence Identities Protection Act of 1982. I recognize
14 that nothing in this Agreement constitutes a waiver by the United
15 States of the right to prosecute me for any statutory violation.

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

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

1 11. I understand that all information to which I may obtain access
2 by signing this Agreement is now and will forever remain the property
3 of the United States Government. I do not now, nor will I ever,
4 possess any right, interest, title, or claim whatsoever to such
5 information. I agree that I shall return all materials which have
6 or may come into my possession or for which I am responsible
7 because of such access, upon demand by an authorized representative
8 of the United States Government or upon the conclusion of my employment
9 or other relationship with the Department or Agency that last
10 granted me either a security clearance or an SCI access approval.
11 If I do not return such materials upon request, I understand that
12 this may be a violation of Section 793, Title 18, United States
13 Code, a United States criminal law.

1 12. Unless and until I am released in writing by an authorized
2 representative of the United States Government, I understand that
3 all conditions and obligations imposed upon me by this Agreement
4 apply during the time I am granted access to SCI and at all times
5 thereafter.

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

1 14. I have read this Agreement carefully and my questions, if any,
2 have been answered to my satisfaction. I acknowledge that the
3 briefing officer has made available to me Sections 641, 793, 794,
4 798, and 952 of Title 18, United States Code, Section 783(b) of
5 Title 50, United States Code, the Intelligence Identities Protection
6 Act of 1982, and Executive Order 12356 so that I may read them at
7 this time, if I so choose.

1 15. I make this Agreement without mental reservation or purpose of
2 evasion.

SIGNATURE _____

DATE _____

SOCIAL SECURITY NUMBER
(SEE NOTICE BELOW)

ORGANIZATION _____

- 1 The execution of this Agreement was witnessed by the undersigned,
- 2 who, on behalf of the United States Government, agreed to its terms
- 3 and accepted it as a prior condition of authorizing access to
- 4 Sensitive Compartmented Information.

WITNESS and ACCEPTANCE:

SIGNATURE _____

DATE _____

ORGANIZATION _____

SECURITY BRIEFING ACKNOWLEDGEMENT

I hereby acknowledge that I was briefed on the following SCI Special Access Program(s):

(Special Access Programs by Initials Only)

Signature of Individual Briefed _____

Date Briefed _____

Printed or Typed Name _____

Social Security Number (See Notice
Below) _____

Organization (Name and Address) _____

I certify that the above SCI access(es) were approved in accordance with relevant SCI procedures and that the briefing presented by me on the above date was also in accordance therewith.

Signature of Briefing Officer _____

Printed or Typed Name _____

Organization (Name and Address) _____

Social Security Number (See Notice
Below) _____

SECURITY DEBRIEFING ACKNOWLEDGEMENT

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the following SCI Special Access Program(s):

(Special Access Programs by Initials Only)

Signature of Individual Debriefed

Date Debriefed

Printed or Typed Name

Social Security Number (See Notice Below)

Organization (Name and Address)

I certify that the debriefing presented by me on the above date was in accordance with relevant SCI procedures.

Signature of Debriefing Officer

Printed or Typed Name

Organization (Name and Address)

Social Security Number (See Notice Below)

- 1 NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal
- 2 agencies inform individuals, at the time information is solicited
- 3 from them, whether the disclosure is mandatory or voluntary, by
- 4 what authority such information is solicited, and what uses will
- 5 be made of the information. You are hereby advised that authority
- 6 for soliciting your Social Security Account Number (SSN) is Executive
- 7 Order 9397. Your SSN will be used to identify you precisely when
- 8 it is necessary to 1) certify that you have access to the information
- 9 indicated above, 2) determine that your access to the information
- 10 indicated has terminated, or 3) certify that you have witnessed
- 11 a briefing or debriefing. Although disclosure of your SSN is not
- 12 mandatory, your failure to do so may impede the processing of such
- 13 certifications or determinations.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name-Printed or Typed)

1 1. Intending to be legally bound, I hereby accept the obligations
2 contained in this Agreement in consideration of my being granted
3 access to classified information. As used in this Agreement, classified
4 information is information that is either classified or classifiable
5 under the standards of Executive Order 12356, or under any other Executive
6 order or statute that prohibits the unauthorized disclosure of information
7 in the interest of national security. I understand and accept that
8 by being granted access to classified information, special confidence
9 and trust shall be placed in me by the United States Government.

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

1 3. I have been advised and am aware that direct or indirect unauthorized
2 disclosure, unauthorized retention, or negligent handling of classified
3 information by me could cause irreparable injury to the United States
4 or could be used to advantage by a foreign nation. I hereby agree
5 that I will never divulge such information unless I have officially
6 verified that the recipient has been properly authorized by the
7 United States Government to receive it or I have been given prior
8 written notice of authorization from the United States Government
9 Department or Agency (hereinafter Department or Agency) last granting
10 me a security clearance that such disclosure is permitted. I
11 further understand that I am obligated to comply with laws and
12 regulations that prohibit the unauthorized disclosure of classified
13 information.

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

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

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

1 7. I understand that all information to which I may obtain access
2 by signing this Agreement is now and will forever remain the property
3 of the United States Government. I do not now, nor will I ever,
4 possess any right, interest, title, or claim whatsoever to such
5 information. I agree that I shall return all materials, which have,
6 or may have, come into my possession or for which I am responsible
7 because of such access, upon demand by an authorized representative
8 of the United States Government or upon the conclusion of my employment
9 or other relationship with the Department or Agency that last
10 granted me a security clearance. If I do not return such materials
11 upon request, I understand that this may be a violation of Section 793,
12 Title 18, United States Code, a United States criminal law.

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

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

1 10. I have read this Agreement carefully and my questions, if
2 any, have been answered to my satisfaction. I acknowledge that
3 the briefing officer has made available to me Sections 641, 793,
4 794, 798, and 952 of Title 18, United States Code, Section 783(b) of
5 Title 50, United States Code, the Intelligence Identities Protection
6 Act of 1982, and Executive Order 12356, so that I may read them
7 at this time, if I so choose.

1 11. I make this Agreement without mental reservation or purpose
2 of evasion.

SIGNATURE

DATE

SOCIAL SECURITY NUMBER
(SEE NOTICE BELOW)

ORGANIZATION

- 1 The execution of this Agreement was witnessed by the undersigned,
- 2 who, on behalf of the United States Government, agreed to its terms
- 3 and accepted it as a prior condition of authorizing access to
- 4 classified information.

WITNESS and ACCEPTANCE:

SIGNATURE

DATE

ORGANIZATION

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



U.S. Department of Justice
Civil Division

Deputy Assistant Attorney General

Washington, D.C. 20530

August 16, 1983

Mr. Robert M. Kimmitt
Executive Secretary
National Security Council
The White House
Washington, D. C. 20506

Re: NSDD-84 Nondisclosure Agreement Forms

Dear Mr. Kimmitt:

In my letter of July 19, 1983, a copy of which is attached, I advised Steven Garfinkel that two draft nondisclosure agreements had been determined by the Department of Justice to be enforceable in civil litigation brought by the United States. Since then, the nondisclosure agreements have been revised, and copies of the final versions are attached to this letter. None of the revisions affect any of the legal analysis contained in my July 19 letter. Therefore, we have concluded that each of the final nondisclosure agreements would be enforceable in accordance with its terms in civil litigation initiated by the United States.

Sincerely,

(Signed)

Richard K. Willard

Richard K. Willard
Deputy Assistant Attorney General

Attachments

cc: Steven Garfinkel



U.S. Department of Justice
Civil Division

Deputy Assistant Attorney General

Washington, D.C. 20530

July 19, 1983

Mr. Steven Garfinkel
Director, Information Security Oversight Office
General Services Administration
Washington, D.C. 20403

Dear Mr. Garfinkel:

Your letter to the Attorney General dated July 1, 1983, requests that the Department of Justice review two nondisclosure agreements drafted pursuant to National Security Decision Directive 84, entitled "Safeguarding National Security Information" (referred to herein as NSDD-84), which was signed by the President on March 11, 1983.

Paragraph 1.a. of NSDD-84 requires all persons with authorized access to classified information to sign a nondisclosure agreement as a condition of access. Paragraph 1.b. imposes the same requirement on persons with authorized access to Sensitive Compartmented Information (SCI) and requires, in addition, that such nondisclosure agreements "include a provision for prepublication review to assure deletion of SCI and other classified information." Paragraph 1.c. provides that the agreements required in paragraphs 1.a. and 1.b. must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States.

We understand that the draft agreements transmitted with your letter were prepared pursuant to the provision in paragraph 1.c. of NSDD-84 that your office develop standardized forms to satisfy the requirements of the directive. We also understand that use of these forms will be mandatory for each agency of the Executive Branch that originates or handles classified information, unless the National Security Council grants permission to use an alternative form of agreement that has been approved by your office and the Justice Department.

Classified Information Nondisclosure Agreement

The essence of the proposed Classified Information Nondisclosure Agreement is an undertaking by the person receiving access to classified information never to disclose such

information in an unauthorized manner. This undertaking is consistent with the provisions of Executive Order 12356, as well as various statutes and other regulations that prohibit the unauthorized disclosure of classified information. In addition, government employees and others who are entrusted with classified information have a fiduciary obligation to protect it from unauthorized disclosure. See Snepp v. United States, 444 U.S. 507, 511 n.6, 515 n.11 (1980).

The protection of national security information is a primary and fundamental constitutional responsibility of the President that derives from his responsibilities as Chief Executive, Commander-in-Chief, and the principal instrument of United States foreign policy. Agreements to preserve the secrecy of classified information are an appropriate method for the President to discharge these constitutional responsibilities. United States v. Marchetti, 466 F.2d 1309, 1315-16 (4th Cir.), cert. denied, 409 U.S. 1063 (1972); cf. Snepp v. United States, supra, 444 U.S. at 509 n.3 (agreement serves "compelling interest" of Government in safeguarding national security information). These same cases also rely upon the statutory authority of the Director of Central Intelligence to protect "intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 403(d)(3). However, the agreements sustained in Marchetti and Snepp were not limited to information concerning intelligence sources and methods but included promises never to disclose any classified information. Therefore, we believe that the President may require the signing of such agreements as a condition of access to classified information.

SCI Nondisclosure Agreement

The proposed SCI Nondisclosure Agreement has the same basic terms as the Classified Information Nondisclosure Agreement discussed above. SCI is a category of classified information that is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods. The power to require signing such an agreement as a condition of access to SCI is thus supported by the statutory authority of the Director of Central Intelligence to protect intelligence sources and methods, 50 U.S.C. § 403(d)(3), as well as the more fundamental constitutional responsibilities of the President regarding national security.

The proposed SCI Nondisclosure Agreement includes provisions for the Government to conduct prepublication review of certain writings by persons who have signed the agreement. The prepublication review provisions of the proposed agreement are similar to the agreement found by the Supreme Court to be enforceable in Snepp v. United States, supra. See also Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362 (4th Cir.), cert. denied, 421 U.S. 992 (1975); United States v. Marchetti, supra; Agee v. CIA, 500 F. Supp. 506 (D.D.C. 1980).

The rationale of the above-cited cases supports the inclusion of prepublication review provisions in agreements that extend beyond CIA to include other persons with authorized access to SCI. Neither the statutory authority of the Director of Central Intelligence nor the constitutional responsibilities of the President are limited to CIA and its employees. Moreover, a high degree of trust, which creates a fiduciary obligation on the part of CIA employees, would also be involved for government officials outside CIA who are entrusted with equally sensitive information such as SCI.

Paragraph 5 of the proposed SCI Nondisclosure Agreement defines the scope of materials required to be submitted for prepublication review. In certain respects, this provision is narrower than the agreement at issue in Snepp. As in the Snepp agreement, however, certain materials must be submitted for review even if they are not thought to contain classified information. The Supreme Court in Snepp upheld the validity of such a requirement. 444 U.S. at 511-13.

Among the categories of materials required in paragraph 5 to be submitted for prepublication review is "(c) any information concerning intelligence activities, sources or methods." This category is not limited to classified information as such, but includes any information that is required to be considered for classification pursuant to Executive Order 12356, § 1.3(a)(4). We believe that agencies using the proposed SCI Nondisclosure Agreement should include in their implementing instructions some definition of the term "intelligence activities," to include at least a reference to the definition contained in Executive Order 12333, § 3.4(e).

Once material is submitted for prepublication review, there is no authority in the proposed agreement for the Government to delete unclassified information. However, any information that is

subject to classification may be deleted pursuant to paragraph 7, even if it does not pertain to SCI or other intelligence matters. See Alfred A. Knopf, Inc. v. Colby, supra, 509 F.2d at 1368-69.

Conclusion

We have reviewed the specific provisions of the two draft agreements transmitted with your letter and have concluded that each would be enforceable in accordance with its terms in civil litigation initiated by the United States.

Sincerely,

(Signed)

Richard K. Willard

Richard K. Willard

Deputy Assistant Attorney General

DEPARTMENT
OF JUSTICE

Order

DOJ 2620.8

Subject: EMPLOYEE OBLIGATIONS TO PROTECT CLASSIFIED INFORMATION
AND SUBMIT TO PREPUBLICATION REVIEW

1. PURPOSE. The purpose of this order is to explain and clarify Department of Justice (DOJ) policies concerning implementation of the prepublication review program.
2. SCOPE. This order applies to all persons granted access to classified information in the course of their employment at the DOJ and DOJ contractors granted such access.
3. AUTHORITY.
 - a. Executive Order 12356, "National Security Information."
 - b. National Security Decision Directive-84 entitled "Safeguarding National Security Information."
 - c. 28 C.F.R. 0.75(p).
4. POLICY. All persons granted access to classified information in the course of their employment at the DOJ are required to safeguard that information from unauthorized disclosure. This nondisclosure obligation is imposed by statutes, regulations, access agreements, and the fiduciary relationships of the persons who are entrusted with classified information in the performance of their duties. The nondisclosure obligation continues after DOJ employment terminates.

As an additional means of preventing unlawful disclosures of classified information, the President has directed that all persons with authorized access to Sensitive Compartmented Information (SCI) be required to sign nondisclosure agreements containing a provision for prepublication review to assure deletion of SCI and other classified information. SCI is information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements

Distribution: BUR/H-1
OBD/F-2 OBD/H-1

Initiated By: Security Staff
Justice Management Division

because it involves or derives from particularly sensitive intelligence sources and methods.

5. RESPONSIBILITIES.

- a. The prepublication review provision requires that DOJ employees granted access to SCI submit certain material to the Department, whether prepared during or subsequent to DOJ employment, prior to its publication to provide an opportunity for determining whether an unauthorized disclosure of SCI or other classified information would occur as a consequence of its publication.

The obligations not to disclose classified information and to comply with agreements requiring prepublication review have been held by the Supreme Court to be enforceable in civil litigation. Snepp v. United States, 444 U.S. 507 (1980).

- b. It must be recognized at the outset that it is not possible to anticipate each and every question that may arise. The Department will endeavor to respond, however, as quickly as possible to specific inquiries by present and former employees concerning whether specific materials require prepublication review. Present and former employees are invited to discuss their plans for public disclosures of information that may be subject to these obligations with authorized Department representatives at an early stage, or as soon as circumstances indicate these policies must be considered. All questions concerning these obligations should be addressed to the Counsel for Intelligence Policy, Office of Intelligence Policy and Review, Room 6325, U.S. Department of Justice, 10th & Constitution Avenue, N.W., Washington, D.C. 20530. The official views of the Department on whether specific materials require prepublication review may only be expressed by the Counsel for Intelligence Policy and persons should not act in reliance upon the views of other Department personnel.
- c. Employees with access to SCI will be required to sign agreements providing for prepublication review. Prepublication review is required only as expressly provided for in an agreement. However, all persons who have had access to classified information have an obligation to avoid unauthorized disclosures of such information and are subject to enforcement actions if they disclose classified information in an unauthorized manner. Therefore, present or former employees are encouraged voluntarily to submit material for

prepublication review if they believe that such material may contain classified information even if such submission is not required by a prepublication review agreement. Where there is any doubt, present and former employees are urged to err on the side of prepublication review to avoid unauthorized disclosures and for their own protection.

- d. Present or former employees who have signed agreements providing for prepublication review are required to submit any material prepared for disclosure to others that contains or purports to contain:
- (1) any SCI, any description of activities that produce or relate to SCI, or any information derived from SCI;
 - (2) any classified information from intelligence reports or estimates; or
 - (3) any information concerning intelligence activities, sources or methods.

The term "intelligence activities" in paragraph 5.d.(3) means all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333. However, there is no requirement to submit for review any materials that exclusively contain information lawfully obtained at a time when the author has no employment, contract, or other relationship with the United States Government and which are to be published at such time.

- e. A person's obligation to submit material for prepublication review remains identical whether such person actually prepares the material or causes or assists another person, such as a ghost writer, spouse or friend, or editor in preparing the material. Material described in paragraph 5.d must be submitted for prepublication review prior to discussing it with or showing it to a publisher, co-author, or any other person who is not authorized to have access to it. In this regard, it should be noted that a failure to submit such material for prepublication review constitutes a breach of the obligation and exposes the author to remedial action even in cases where the published material does not actually contain SCI or classified information. See Snepp v. United States, supra.

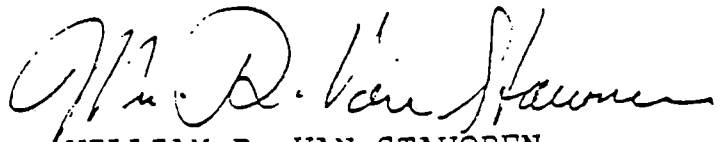
- f. The requirement to submit information or materials for prepublication review is not limited to any particular type of material or disclosure. Written materials include not only books but all other forms of written materials intended for public disclosure, such as (but not limited to) newspaper columns, magazine articles, letters to the editor, book reviews, pamphlets, and scholarly papers. Because fictional treatment may convey factual information, fiction is also covered if it is based upon or reflects information described in paragraph 5.d.
- g. Oral statements are also included when based upon written materials, such as an outline of the remarks. There is no requirement to prepare such material for prior review, however, unless there is reason to believe in advance that oral statements may contain SCI or other classified information. Thus, a person may participate in an oral presentation of information where there is no opportunity for prior preparation (e.g., news interview, panel discussion) unless there is reason to believe in advance that such oral expression may contain SCI or other classified information. This recognition of the problems with oral representations does not, of course, exempt present or former employees from liability for any unauthorized disclosures of SCI or classified information that may occur in the course of even extemporaneous oral expressions.
- h. Material that consists solely of personal views, opinions or judgments and does not contain or imply any statement of fact that would fall within the description in paragraph 5.d is not subject to the prepublication review requirement. For example, public speeches or publication of articles on such topics as proposed legislation or foreign policy do not require prepublication review as long as the material does not directly or implicitly constitute a statement of an informational nature that falls within paragraph 5.d. Of course, in some circumstances the expression of "opinion" may imply facts and thus be of such a character as to require prior review.
- i. Obviously, the purposes of prepublication review will be frustrated where the material in question already has been disseminated to unauthorized persons. Comparison of the material before and after the review would reveal which items of classified information, if any, had been deleted at the Department's request. Consequently, the Department will consider these obligations to have been breached in any case, whether or not the written material is subsequently

submitted to the Department for prepublication review, where it already has been circulated to publishers or reviewers or has otherwise been made available to unauthorized persons. While the Department reserves the right to review such material for purposes of mitigating damage that may result from the disclosure, such action shall not prevent the United States Government and the Department from pursuing all appropriate remedies available under law as a consequence of the failure to submit the materials for prior review and/or any unauthorized disclosure of SCI or classified information.

- j. Materials submitted for prepublication review will be reviewed solely for the purpose of identifying and preventing the disclosure of SCI and other classified information. This review will be conducted in an impartial manner without regard to whether the material is critical or favorable to the Department. No effort will be made to delete embarrassing or critical statements that are unclassified. Materials submitted to the Office of Intelligence Policy for review will be disseminated to other persons or agencies only to the extent necessary to identify classified information.
- k. The Counsel for Intelligence Policy will respond substantively to prepublication review requests within 30 working days. Priority shall be given to reviewing speeches, newspaper articles, and other materials that the author seeks to publish on an expedited basis. The Counsel's decisions may be appealed to the Deputy Attorney General, who will process appeals within 15 working days. The Deputy Attorney General's decision is final and not subject to further administrative appeal. Authors who are dissatisfied with the final administrative decision may obtain judicial review either by filing an action for declaratory relief or by giving the Department notice and a reasonable opportunity (30 working days) to file a civil action seeking a court order prohibiting disclosure. Of course, until any civil action is resolved in court, employees remain under an obligation not to disclose or publish information determined by the Government to be classified.
- l. Nothing in this order should be construed to alter or waive the Department's authority to seek any remedy available to it to prohibit or punish the unauthorized disclosure of classified information.

;

- m. A former DOJ employee who subsequently receives a security clearance or SCI access approval from another department or agency is permitted to satisfy any obligation regarding prepublication review by making submissions to the department or agency that last granted the individual either a security clearance or an SCI access approval.
- n. The obligations described herein as applying to DOJ employees also apply with equal force to contractors who are authorized by the Department to have access to SCI or other classified information.



WILLIAM D. VAN STAVOREN
Acting Assistant Attorney General
for Administration

United States Senate

WASHINGTON, D.C. 20510

January 10, 1984

Ms. Brenda S. Reger
National Security Council Director
Office of Information Policy
and Security Review
Old Executive Office Building, Room 375
Washington, D.C. 20506

Dear Ms. Reger:

Could you please send my Los Angeles office a copy of
the following:

National Security Directive: Pre-Publication Review

The address is:

11000 Wilshire Blvd., Suite 11221
Los Angeles, CA 90024
Attn: Mr. Don Ediger

Thank you so much. Your attention to this matter would
be greatly appreciated.

Sincerely,



PETE WILSON
United States Senator

PW/csr

MEMORANDUM

NATIONAL SECURITY COUNCIL

July 25, 1983

INFORMATION

MEMORANDUM FOR THE NSC STAFF

FROM: ROBERT M. KIMMITT *Bh*

SUBJECT: Security

Effective today, Paul Thompson has assumed primary responsibility for security on the National Security Council Staff, including investigations, background checks, and clearances (collateral and compartmented). Inquiries on these subjects henceforth should be directed to Paul (extension 3046) rather than Dick Morris or Kathleen Shanahan.

There have been recent instances of security violations on the Staff, generally involving the failure to secure classified material in the evening. Each office's security procedures should be reviewed to ensure double checks whenever possible. Paul Thompson has been asked to submit a report to me on each future violation, to include written statements from those involved in the violation.

We would welcome any suggestions you may have on improving NSC security, an important task for which we all share responsibility.

THE WHITE HOUSE

WASHINGTON

ACTION

February 28, 1981

MEMORANDUM FOR: NSC STAFF

FROM: RICHARD V. ALLEN *lon*

SUBJECT: Contacts with Diplomatic and Official
Representatives of Soviet, East European,
People's Republic of China, and Cuban
Governments in the United States

The following procedures should be observed by NSC Staff Officers in making contacts within the United States with diplomatic and other official representatives of subject governments:

- In advance of each proposed contact, you should notify my office as to the purpose you expect to derive from the contact, and specify the hour, date and place of the meeting, and furnish a copy of the memo to the NSC Security Office.
- After the contact has been made, submit a memo to my office covering any policy matters of substance that may have been discussed.

Adherence to these procedures will facilitate the coordination and consideration of matters of national security interest that may arise in the areas of contact made outside the usual diplomatic and public channels.

DRAFT

Dear

The President has asked me to respond to your letter about National Security Decision Directive 84 (NSDD-84).

The President issued NSDD-84 because of serious concern about the damage to intelligence sources caused by unauthorized disclosures of classified information. Both anonymous leaks to the press and unauthorized disclosures in the writings of former officials have caused losses of sensitive intelligence information. This has been a problem in past administrations as well, prompting the congressional intelligence committees to urge more vigorous action in investigating and prosecuting leak cases.

Following the adoption of NSDD-84 in March of last year, however, various Members of Congress expressed concern about two provisions of the directive: paragraph 1(b), which authorized broader use of prepublication clearance agreements, and paragraph 5, relating to the use of the polygraph in leak investigations. Amendments to the State and Defense Authorization bills were adopted last year barring the Administration from implementing either of these two proposals until April 15 of this year.

Rather than resume the legislative debate on the merits of NSDD-84, the Administration has sought to work cooperatively with Congress to develop a mutually-acceptable solution to this problem. For this reason, the two controversial provisions have been suspended indefinitely.

Unfortunately, the article by Carl Rowan in the April issue of Reader's Digest contains serious factual inaccuracies about the President's directive as well as other matters relating to the protection of classified information. The enclosed fact sheet should help to set the record straight.

Sincerely,

March 30, 1984

Fact Sheet on Carl Rowan's Article,
"Mr. President, This Isn't Russia."
Reader's Digest, April, 1984, p. 65

Prepublication Review

Rowan says: The March 1983 directive is absurd because it would require prepublication review for George Schultz's memoirs, Jeane Kirkpatrick's foreign policy speeches as a 1988 Vice-Presidential candidate, or a letter to the editor by a retired Marine Commandant.

The facts: Prepublication review is not a new concept. ^{among others,} Henry Kissinger, Cyrus Vance, Zbigniew Brezinski, and Alexander Haig have submitted books and articles for prepublication review. George Bush was able to run for Vice-President in 1980, having previously signed such an agreement as Director of Central Intelligence.

* * *

Rowan says: A law professor from the University of Texas believes that prepublication review is forbidden by the Constitution.

The facts: The Supreme Court upheld the constitutionality of CIA's prepublication review requirement in Snepp v. United States (1980). Mr. Rowan's article does not even mention this landmark Supreme Court decision.

* * *

Rowan says: The directive requires submitting to a censor "all writings on foreign policy or defense," as well as discussions of intelligence matters.

The facts: Writings on foreign policy or defense would not have to be submitted for review, unless they contain information derived from or relating to specified intelligence matters.

* * *

Rowan says: This program will allow the Administration in power to suppress the views of former officials who are critical of its policies.

The facts: Only classified information can be deleted from materials that are submitted for review. Judicial review is provided, and the government must be able to prove in court that any deleted material is properly classified.

* * *

Rowan says: Even though prepublication review is supposed to be completed within 30 days, this clearance process is so cumbersome as to stifle expert commentary on critical events from non-government sources.

The facts: Last year, CIA's prepublication review board considered 213 submissions and the average clearance time was 13 days. Reviews have been conducted in a matter of hours for authors working on short deadlines.

* * *

FOIA Amendments

Rowan says: In October 1981 the Administration asked Congress to "gut" the Freedom of Information Act.

The facts: The Administration supports two bills to reform FOIA, neither of which would "gut" the Act. The general FOIA reform bill is S. 774, which would (among other things) improve the protection of information in law enforcement files. The Administration also supports S. 1324, which would exempt certain CIA operational files from FOIA. Both bills have passed the Senate with strong bipartisan support--indeed, without a dissenting vote.

* * *

Executive Order on Classification

Rowan says: In April 1982, President Reagan issued a new Executive Order that "made it almost mandatory for bureaucrats to put secrecy classifications on more documents."

The facts: Statistics recently compiled by the Information Security Oversight Office (ISOO) show that the new order has not produced an increase in the amount of classified information. During the first year that the new order was in effect (FY 1983), original classification declined by 18%. Total classification activity (including derivative classification) increased by only 3%, which is much lower than 8-10% annual increases during the last two years of the Carter Administration.

* * *

Rowan says: The new order eliminated the requirement that some "identifiable potential harm to national security" had to be demonstrated inside the government before information could be classified." (Emphasis in original.)

The facts: The new order requires that information can be classified only if its unauthorized disclosure "reasonably could be expected to cause damage to the national security." This order eliminated the requirement, which was imposed for the first time in the Carter Administration, that "identifiable damage" must be shown. Incidentally, this standard is not one that is applied only inside the Administration, since under the Freedom of Information Act all classification decisions are subject to de novo judicial review.

* * *

Rowans says: The new order requires "officials with any doubt to classify materials at the highest rather than the lowest possible level of secrecy."

The facts: The order says: "If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days."

* * *

Rowan says: The new order gives officials the power to reclassify information that has been made public, which serves no legitimate purpose.

The facts: The order allows information to be reclassified only under a stringent set of circumstances. The purpose of this provision, which has rarely been applied, is to permit the government to countermand an unwise decision to declassify if the information in question has not been widely disseminated. Otherwise, declassification decisions would be irrevocable--regardless of the resulting harm to national security.

* * *

Canadian Films

Rowan says: In January 1983 the Administration tried to discredit some films produced by the Canadian government because they dealt with controversial environmental issues.

The facts: Career employees of the Justice Department simply applied the Foreign Agents Registration Act of 1938 to these films, in the same way that this law had been applied in prior administrations. A federal judge has recently held the statute unconstitutional, but his opinion indicated that Congress had intended the statute to cover films such as these. (The statute, by the way, does not restrict dissemination of the films, but merely requires an identifying label.)

* * *

Polygraphs

Rowan says: The directive calls for expanded use of lie detectors. An employee who refused to take a polygraph test could be disciplined or even fired.

The facts: The Administration has taken the position that employees with civil service protection would not be fired or demoted for refusing to take a polygraph test. However, where these employees deal with highly classified information, they could be moved to less sensitive positions at the same salary level. CIA and NSA have used polygraph examinations as part of their security program for many years. Consideration has been given to expanding use of the polygraph to a small number of additional jobs that are of exceptional interest to hostile intelligence services. This

is primarily a counter-espionage program rather than an anti-leak measure.

* * *

Rowan says: The congressional Office of Technology (OTA) says that "there is no scientific evidence to support the use of lie detectors for screening large numbers of people, as in an investigation for leaks"

The facts: Although the OTA study found no scientific evidence of polygraph validity for large-scale screening, it did not apply this conclusion generally to leak investigations. The OTA did find scientific evidence of polygraph validity in criminal investigations. In fact, OTA concluded: "[T]o the extent polygraph use in unauthorized disclosure investigations is similar to the way the polygraph is used in criminal investigations, there is at least some although far from conclusive scientific basis for polygraph validity."

* * *

Conclusions

Rowan says: President Reagan, because of "his oft-stated fear of Communism," is attempting to impose security restrictions that "will in fact make America more and more like Communist regimes he so abhors."

The facts: Nothing the President has proposed will change the fact that this is the most open society, with the freest press, in the world. Many other democratic countries--such as Britain and Sweden--have much stricter official secrecy laws than the United States. Too much secrecy is obviously bad, but when it comes to intelligence and military matters, some secrecy is necessary and indeed vital to our ability to live in peace and freedom.

* * *

Rowan says: Even though President Reagan has held up on implementing the most controversial provisions of NSDD-84, Congress should refuse to compromise on these issues. Indeed, the Directive should be completely withdrawn.

The facts:

Most of the Directive's provisions have nothing to do with prepublication review or polygraphs, and have not been criticized by Congress. Rowan has articulated no reason ~~in the world~~ to withdraw these non-controversial provisions of the Directive. Congress should act on the recommendations of its own intelligence committees (which have criticized the failure to solve leak cases) and devise a legislative solution to this problem.

63RD YEAR

Reader's Digest

APRIL 1984

An article a day of enduring significance, in condensed permanent booklet form

Mr. President, This Isn't Russia



The Reagan Administration's Directive 84—which features lie-detector tests, secrecy oaths and censorship for life—would threaten the very freedoms it seeks to keep secure. It should be completely withdrawn—for good

IF SECRETARY of State George Shultz ever writes his memoirs—telling us how the United States got involved in Lebanon, say, or why arms-control talks with the Soviet Union went sour—he would have to submit his manuscript to a government review board for approval.

If Jeane Kirkpatrick, the U.S. Permanent Representative to the United Nations, were to become a candidate for Vice President in

BY CARL T. ROWAN

CARL T. ROWAN, a Reader's Digest Roving Editor, is a former Deputy Assistant Secretary of State, Ambassador to Finland and Director of the U.S. Information Agency.

1988, she would have to clear her foreign-policy speeches with a federal censor who just might be working for an Administration she wants to throw out of office.

Or if, a few years from now, the retired Marine who was Commandant during our years of involvement in Lebanon wants to write a letter to a newspaper spelling out booby traps that ought to be avoided by his successor, a government censor would have the power to tell him just what he may or may not say.

Does all this sound absurd? Well, it is the real world of Washington 1984. Last year President Reagan issued a highly controversial order, called Directive 84, which among other things would impose *lifetime pre-publication censorship* on federal officials who have had access to highly classified information.

Small wonder, then, that Directive 84 has aroused a storm of protest. "If this directive had been issued under a liberal, Democratic government," one of Reagan's own senior foreign-policy officials told me, "conservative Republicans would be crying from the rooftops." The American Society of Newspaper Editors calls it "peace-time censorship of a scope unparalleled in this country since the adoption of the Bill of Rights." Veteran NBC newsman and former Voice of America Director John Chancellor calls the action "the most sweeping and dictatorial

censorship directive in the history of the American government." The American Civil Liberties Union characterizes it as "a frontal assault against First Amendment values and, ultimately, democracy itself."

"No matter how pure the goal is," sums up Lucas A. Powe, Jr., law professor at the University of Texas, "there are some means that cannot be used consistent with our Constitution. A system of prior censorship is one of those forbidden means. If the national interest is harmed by disclosure, then punish those who disclose. But do not punish all Americans by subjecting thousands of their fellow citizens to a regime of perpetual censorship."

Broad Pattern. In all fairness, even the sternest critics of Directive 84 are not saying that the President deliberately wants to impose a White House dictatorship upon this society. *All* Presidents have insisted, quite rightly, that vital national secrets must be kept safe from unwarranted disclosure. What critics *are* saying is that this President, in his oft-stated fear of Communism, is trying to make the United States "more secure" by infringing upon traditional freedoms in ways that will in fact make America more and more like the Communist regimes he so abhors.

Concern has been generated not solely by Directive 84, but by a broader pattern of more government secrecy and less public access

1984.

MR. PRESIDENT, THIS ISN'T RUSSIA

to information vital to informed decision-making in a democracy. Consider:

- In October 1981 the Administration asked Congress to gut the Freedom of Information Act (FOIA). This law, enacted in 1966 and strengthened by Congress in 1974 after the Watergate scandals, gave the American people the right to know what the government was filing about them or doing to them, their relatives and neighbors. It became a symbol of open and honest government in America.

There is evidence that America's enemies, including the Soviet KGB, have used the FOIA to get helpful information, and surely some refinements of the law are called for. But the Reagan Administration—acting as though it wants to return to the excessive secrecy that allowed massive abuses and violations of law by the FBI, CIA and other agencies during the 1960s and early 1970s—has been trying to limit FOIA's scope and make it more difficult and expensive for citizens to get information.

- On April 2, 1982, President Reagan issued an Executive Order on Classification that reversed a 30-year trend and made it almost mandatory for bureaucrats to put secrecy classifications on more documents. The order wiped out the requirement that some *identifiable potential harm to national security* had to be demonstrated inside the government before information could be classified, and it ordered officials

with any doubt to classify materials at the highest rather than the lowest possible level of secrecy.

In addition, government officials got expanded power to *reclassify* information that had already been made public. What possible good can this do? Its major effect is to discourage journalists and others from trying to get material under the FOIA. "Sorry," authorities can say, "that material has just been reclassified 'top secret.'"

- In January 1983 the Administration tried to discredit films produced by the National Film Board of Canada because they dealt with such themes as the effects of nuclear war and the impact of acid rain. In response, Congressman Jim Leach (R., Iowa) said, "It may be too extreme to label this a harbinger of McCarthyism, but it sends a chilling message to all Americans, especially those deeply concerned about environmental issues in general and about the ultimate environmental issue—the survival of the planet."

- Along with pre-publication review, Directive 84 calls for expanded use of lie detectors to check on federal employees. Almost half of the federal civilian and military work force, some 2.5 million men and women, along with 1.5 million employees of defense contractors, would be required to take polygraph examinations in investigations of unauthorized disclosures. In addition, 128,000 workers with access to Sensitive Compartmented

Information—the really super secrets—could be required to take polygraph tests on a *random* basis; i.e., not just when leaks are suspected, but *any time at all*. If an employee refused to take a lie-detector test, he or she could be disciplined or even fired.

Yet Congress's Office of Technology Assessment has reported that there is no scientific evidence to support the use of lie detectors for screening large numbers of people, as in an investigation for leaks, and that such use carries a high risk of misidentifying many innocent people as liars.

Lifetime Vow. But of all the steps taken by the Reagan White House to block the flow of information, the most alarming and outrageous has been its attempt to extend throughout the Executive branch the lifetime censorship now imposed only on CIA and National Security Agency employees. Directive 84 would require that any employee with access to Sensitive Compartmented Information must sign a contract pledging to submit for review by a government censor all writings on foreign policy and defense, or anything that might allude to "intelligence activities, sources or methods," even if the material is not classified. The contract covers books, novels, magazine articles, speeches—virtually *everything*. And it is in force not only while the person is working for the government but also after he or she leaves. It is a lifetime vow.

68

The implications of the directive are mind-boggling. Had such a requirement been issued by Harry Truman, for example, books, articles and speeches by Dean Acheson, Douglas MacArthur and George Kennan, to name just a few, would have been subject to pre-publication review (in some cases by censors working for a different Administration). The rule would put journalists who have served in government—the likes of Bill Moyers, William Safire, John Chancellor and, yes, Carl Rowan—in the absurd position of having to get the prior approval of the very people they want to criticize in their columns or commentaries.

Lawyers say the confusion, silliness and unworkability of Directive 84 are manifest in language suggesting that a former high official using notes for a college lecture, TV appearance or testimony before Congress would have to submit them for censorship. But that official could avoid censors and reveal anything if speaking extemporaneously. Another galling bit of irony is that the President, Vice President and members of Congress, the most active leakers in Washington, would be exempt from Directive 84 because they are *elected*. So they could continue to get rich writing about secret data and developments.

"Powerful Impact." A recent survey of five leading newspapers—the New York Times, Washington Post, Los Angeles Times, The Wall Street Journal and The Christian Sci-

1984,

MR. PRESIDENT, THIS ISN'T RUSSIA

ence Monitor—found that those newspapers published more than 300 articles in 1982 written by current or former government officials, most of which would have been covered by the pre-publication-review requirement had it been in effect at the time. Among those whose works would have been affected were four ex-Secretaries of State, two former Secretaries of Defense, two ex-national security advisers, along with former ambassadors, arms-control specialists and weapons experts. The subjects covered included the MX missile, U.S. Central American policy, military spending, Soviet intelligence gathering, the Middle East crisis and the situation in Poland.

"This indicates the powerful impact the measure could have," says Patricia Derian, one-time Assistant Secretary of State. "The views of these former officials are vital if reasonable public debate is to take place."

The review board is supposed to act within 30 days and to remove only sensitive material. But even if everything in a particular document is okayed, the clearance procedure is so cumbersome and slow as to risk making it irrelevant. As a result, there might have been no immediate expert commentary on such critical topics as last year's invasion of Grenada, the downing of Korean Flight 007, or Marine deaths in Lebanon—except from official government sources. This, in effect, allows government to sup-

press the views of opponents and thereby dominate public debate.

Right to Know. Numerous officials and former officials have testified that in the last quarter-century there has been not even a handful of nation-threatening leaks. Why, then, has the Reagan Administration gone to such extremes?

"Our government's ability to protect vital secrets is not adequate today," says Acting Assistant Attorney General Richard K. Willard, who headed the task force that recommended the policies of Directive 84. "In the wake of Watergate and Vietnam," he told an ABC "Nightline" audience last January, "there was a great trend toward openness in government—uncovering secrets. But during the seventies the pendulum, we think, swung too far. We're trying to restore some of that balance."

Willard doesn't claim that the new rules will halt all leaks, but he thinks they will "change the attitudes of government officials." And the President himself has said, "With regard to national security, we're not doing anything that I think unfairly imposes a restriction on the right of the people to know."

There are many, however, who think the new regulations *would* restrict the people's right to know. And more: these critics see a purposeful attempt to manage the news and control the truth, arising out of the Administration's misconceptions about govern-

READER'S DIGEST

ment's responsibility in a democratic society.

President Reagan and the admirals and generals he commands must accept the fact that the presence of news people in Lebanon, or Grenada, or wherever, is not a government *favor* to the press. It is a way of saying to the American people: "We in the White House are accountable to *you* who gave us political power. We in the Pentagon are accountable to *you* who gave us military power. You cannot all be in these places to make individual judgments as to whether we are using those powers wisely. Therefore, we accept a free press as our citizens' eyes and ears."

To prevent President Reagan from enforcing Directive 84, Congress voted last October to delay the pre-publication-review provisions for six months, and early this year began considering legislation to overturn the directive permanently. Although the President has argued that he does not need Congressional approval to enforce his censorship scheme, a growing number of Republicans and Democrats have insisted that if the President did not withdraw it, Congress should legislate against it

directly. Under this bipartisan pressure, the White House announced in mid-February that the President would hold up implementation of the most controversial portions of Directive 84—those imposing lifetime pre-publication censorship and calling for wider use of lie detectors—until he reaches a compromise with Congress.

But there must be no "compromise" that embraces a fundamental erosion of freedom. This society has survived assaults by every conceivable enemy of democracy without renouncing the liberties secured, not just on parchment, but in the hearts of generations of Americans. No threat of any sort ought to make us act like totalitarians in the foolish notion that this is how we remain free.

YOU CAN HAVE A SAY ON this critical issue by exercising your right of free expression. Write to President Reagan. Urge him to withdraw Directive 84 *completely* and to forget about ever implementing anything remotely resembling its most threatening sections. Your voice, joined by countless other voices, can make a difference.

For information on reprints of this article, see page 230.

*P*UBLIC NOTICE in the New York Times: "To my lovely wife, M. Thank you for 50 wonderful years of married life together—except for the argument we had in 1935 in which you were obviously wrong. Love, husband M. B."

Digest Editor Resigns

By DAVID E. SANGER

The editor in chief of Reader's Digest, Edward T. Thompson, resigned Friday because of what the company called "fundamental differences of editorial philosophy" with the magazine's board of directors.

His successor, effective immediately, will be Kenneth O. Gilmore, the magazine's executive editor and vice president of the Reader's Digest Association, the privately held parent company of the publication.

A spokesman for the association would not elaborate on the reasons for Mr. Thompson's sudden departure, other than to say that his differences were with "representatives of Lila Acheson Wallace," who owns all of the voting shares in the company. There was no answer yesterday at Mr. Thompson's home in Bedford, N.Y. The spokesman said that Mr. Thompson, who is 56 years old and has edited the magazine for eight years, would take early retirement.

Mr. Gilmore, 53, was also elected a director of the Reader's Digest Association on Friday, and a member of its executive committee. Reached yesterday at his home in Mt. Kisco, N.Y., Mr. Gilmore said that "I think it will be a tremendous challenge to continue to carry on the job of providing our readers here and abroad with the kind of magazine content that enriches their lives and engenders such unwavering loyalty." He declined to discuss the circumstances that led to Mr. Thompson's resignation.

Mr. Gilmore, who said yesterday that he plans no major changes at the

magazine, joined Reader's Digest 27 years ago. He started as a researcher and then was a writer in the magazine's Washington bureau. In 1968, he was made bureau chief.

He moved to the magazine's headquarters in Chappaqua, N.Y., in 1973 as an assistant managing editor, and two years later became a managing editor. He assumed his role as executive editor in May 1982.

Until recently, he was primarily responsible for Reader's Digest's international editions, which have a circulation of about 12 million, compared with 18 million in the United States, Mr. Gilmore said. While supervising the international editions, he played a major role in the magazine's publication of "The Pope to Murder the Pope," an August 1982 article by Claire Sterling that charged that the Soviet Union was involved in the assassination attempt on Pope John Paul II in May 1981.

In fact, covert action by the Soviet Union has been a particular interest of Mr. Gilmore's. In 1962 he co-authored "The Great Deception," a book he described yesterday as "telling how the Kremlin took Cuba." He also edited two books on the K.G.B., the Soviet Government's intelligence and internal-security agency, written by John Barron and published by Reader's Digest. Mr. Gilmore was also the editor of President Ford's memoir, "A Time to Heal."

Mr. Gilmore graduated from Brown University in 1953. He is a member of the Council on Foreign Relations in New York and an adviser to the Georgetown University Center for Strategic and International Studies.

ISOO ANNUAL REPORT ON THE INFORMATION SECURITY PROGRAM

- Q. When issuing E.O. 12356, one of its major purposes was to improve protection for national security information. You later issued NSDD-84 because purportedly there were problems with "leaks" of information. Does this mean that your executive order has failed in accomplishing its purpose?
- A. The order establishes an overall system for the classification, declassification, and safeguarding of national security information. "Leaks" are conscious decisions by individuals to violate the protective requirements established by this system. They have been experienced under other executive orders as well. NSDD-84 was an effort to bring attention to a continuing problem and to establish procedures to improve protection of our national security information.

ISOO ANNUAL REPORT ON THE INFORMATION SECURITY PROGRAM

- Q. This report places great stress on the fact that there was a decrease in original classification. Why does it seem to ignore the fact that derivative classification, which is 95 percent of all classification, increased in FY 1983?
- A. Most derivative classification decisions made in FY 1983 are a result of original classification decisions made in prior years. Because an original classification action results, on the average, in 19 derivative actions, it is imperative that the number of original classifications be limited. Decreased original classification ultimately results in fewer derivative classification decisions. The number of original classification decisions is the most important measurement of an information security program.

ISOO ANNUAL REPORT ON THE INFORMATION SECURITY PROGRAM

- Q. There has been a significant decline in the systematic review program over the past few years. What can be done to speed up the process by which the public, historians, and the media learn about the affairs of government?
- A. E.O. 12356 acknowledged that systematic review at the National Archives and Records Service (NARS) remains the most cost effective means of declassifying large quantities of records in greatest demand by researchers. The decrease in systematic review activity over the past few years is not a result of the information security system in place. Rather, its decline can be attributed to two factors. First, the resources available for systematic review at NARS have shrunk, the result of both redefined agency priorities and overall budget cuts. Second, the subject matter of the records that are now being reviewed is not generally susceptible to the bulk declassification methods that were easily applied to World War II records. The President has expressed his support for this effort and has asked ISOO and responsible government officials to pay particular attention to this effort.

ISOO ANNUAL REPORT ON THE INFORMATION SECURITY PROGRAM

- Q. What about the situation (any specific allegation or reference to a particular case, as for example, the State Department's shipment of classified records to Lorton Reformatory, or the National Security Agency's efforts to reclassify information in the George C. Marshall Library)?
- A. The report notes such instances among the aggregate figures it reflects since the Information Security Oversight Office is responsible for oversight of such matters. Details on specific cases should be addressed to ISOO or to the agency in question.

Digest Editor Resigns

By DAVID E. SANGER

The editor in chief of Reader's Digest, Edward T. Thompson, resigned Friday because of what the company called "fundamental differences of editorial philosophy" with the magazine's board of directors.

His successor, effective immediately, will be Kenneth O. Gilmore, the magazine's executive editor and vice president of the Reader's Digest Association, the privately held parent company of the publication.

A spokesman for the association would not elaborate on the reasons for Mr. Thompson's sudden departure, other than to say that his differences were with "representatives of Lila Acheson Wallace," who owns all of the voting shares in the company. There was no answer yesterday at Mr. Thompson's home in Bedford, N.Y. The spokesman said that Mr. Thompson, who is 56 years old and has edited the magazine for eight years, would take early retirement.

Mr. Gilmore, 53, was also elected a director of the Reader's Digest Association on Friday, and a member of its executive committee. Reached yesterday at his home in Mt. Kisco, N.Y., Mr. Gilmore said that "I think it will be a tremendous challenge to continue to carry on the job of providing our readers here and abroad with the kind of magazine content that enriches their lives and engenders such unwavering loyalty." He declined to discuss the circumstances that led to Mr. Thompson's resignation.

Mr. Gilmore, who said yesterday that he plans no major changes at the

magazine, joined Reader's Digest 27 years ago. He started as a researcher and then was a writer in the magazine's Washington bureau. In 1963, he was made bureau chief.

He moved to the magazine's headquarters in Chappaqua, N.Y., in 1973 as an assistant managing editor, and two years later became a managing editor. He assumed his role as executive editor in May 1982.

Until recently, he was primarily responsible for Reader's Digest's international editions, which have a circulation of about 12 million, compared with 18 million in the United States, Mr. Gilmore said. While supervising the international operations, he played a major role in the magazine's publication of "The Pope So Murder the Pope," an August 1982 article by Claire Sterling that charged that the Soviet Union was involved in the assassination attempt on Pope John Paul II in May 1981.

In fact, covert action by the Soviet Union has been a particular interest of Mr. Gilmore's. In 1962 he co-authored "The Great Deception," a book he described yesterday as "telling how the Kremlin took Cuba." He also edited two books on the K.G.B., the Soviet Government's intelligence and internal-security agency, written by John Barron and published by Reader's Digest. Mr. Gilmore was also the editor of President Ford's memoir, "A Time to Heal."

Mr. Gilmore graduated from Brown University in 1953. He is a member of the Council on Foreign Relations in New York and an adviser to the Georgetown University Center for Strategic and International Studies.

Interesting!

Fact Sheet on Carl Rowan's Article,
"Mr. President, This Isn't Russia."
Reader's Digest, April, 1984, p. 65

Prepublication Review

Rowan says: The March 1983 directive is absurd because it would have required prepublication review for George Schultz's memoirs, Jeane Kirkpatrick's foreign policy speeches as a 1988 Vice-Presidential candidate, or a letter to the editor by a retired Marine Commandant.

The facts:

PPR is not a new concept. Among others,
Henry Kissinger, Cyrus Vance, *and Alexander Haig* and Zbigniew Brezinski submitted ~~their memoirs~~ for prepublication review, *and Alexander Haig have* prior to promulgation of *+ for article* this directive. George Bush was able to run for Vice-President in 1980, having previously signed such an agreement as Director of Central Intelligence.

* * *

Rowan says: A law professor from the University of Texas believes that prepublication review is forbidden by the Constitution.

The facts:

The Supreme Court upheld the constitutionality of CIA's prepublication review requirement in Snepp v. United States (1980). ~~It is incredible that~~
7th. Rowan ~~could~~ write a lengthy article ~~on~~ *concerning* prepublication review without even mentioning this landmark Supreme Court decision.

* * *

Rowan says: The directive requires submitting to a censor "all writings on foreign policy or defense," as well as discussions of intelligence matters.

The facts:

Writings on foreign policy or defense would not have to be submitted for review, unless they contain information relating to specified intelligence matters.

* * *

Rowan says: This program will allow the Administration in power to suppress the views of former officials who are critical of its policies.

The facts: Only classified information can be deleted from materials that are submitted for review. Judicial review is provided, and the government must be able to prove in court that ~~it wants to take out~~ *deleted info* is properly classified.

* * *

Rowan says: Even though prepublication review is supposed to be completed within 30 days, this clearance process is so cumbersome as to stifle expert commentary on critical events from non-government sources.

The facts: Last year, CIA's prepublication review board considered 213 submissions and the average clearance time was 13 days. Reviews have been conducted in a matter of hours for authors working on short deadlines.

* * *

FOIA Amendments

Rowan says: In October 1981 the Administration asked Congress to "gut" the Freedom of Information Act.

The facts: The Administration supports two bills to reform FOIA, neither of which would "gut" the Act. *Come, in* The general FOIA reform bill is S. 774, which would (among other things) improve the protection of information in law enforcement files. *The* ~~The Administration also supports S. 1324, which would exempt certain CIA operational files from FOIA.~~ Both bills have passed the Senate on voice votes, with strong bipartisan support--indeed, without a dissenting vote. *and the other*

* * *

Executive Order on Classification

Rowan says: In April 1982, President Reagan issued a new Executive Order that "made it almost mandatory for bureaucrats to put secrecy classifications on more documents."

The facts: Statistics recently compiled by the Information Security Oversight Office (ISOO) show that the new order has not produced an increase in the amount of classified information. During the first year that the new order was in effect (FY 1983), original classification declined by 18%. Total classification activity (including derivative classification) increased by only 3%, which is much lower than 8-10% annual increases during the last two years of the Carter Administration.

* * *

Rowan says: The new order eliminated the requirement that some "identifiable potential harm to national security had to be demonstrated inside the government before information could be classified." (Emphasis in original.)

The facts: The new order requires that information can be classified only if its unauthorized disclosure "reasonably could be expected to cause damage to the national security." This order eliminated the requirement, which was imposed for the first time in the Carter Administration, that "identifiable damage" must be shown. Incidentally, this standard is not one that is applied only inside the Administration, since under the Freedom of Information Act all classification decisions are subject to de novo judicial review.

* * *

Rowans says: The new order requires "officials with any doubt to classify materials at the highest rather than the lowest possible level of secrecy."

The facts: The order says: "If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days."

* * *

Rowan says: The new order gives officials the power to reclassify information that has been made public, which serves no legitimate purpose.

The facts:

The order allows information to be reclassified *under a stringent set of circumstances* only if it (a) requires protection in the interest of national security and (b) may reasonably be recovered. ~~Where declassified information has received any substantial public dissemination, it is not reasonably recoverable and thus cannot be reclassified.~~ The purpose of this provision, which has rarely been applied, is to permit the government to countermand an unwise decision to declassify if the information in question has not been widely disseminated. Otherwise, declassification decisions would be irrevocable-- regardless of the resulting harm to national security.

* * *

Canadian Films

Rowan says:

In January 1983 the Administration tried to discredit some films produced by the Canadian government because they dealt with controversial environmental issues.

The facts:

Career employees of the Justice Department simply applied the Foreign Agents Registration Act of 1938 to these films, in the same way that this law had been applied in prior administrations. A federal judge has recently held the statute unconstitutional, but his opinion indicated that Congress had intended the statute to cover films such as these. (The statute, by the way, does not restrict dissemination of the films, but merely requires an identifying label.)

* * *

Polygraphs

Rowan says:

The directive calls for expanded use of lie detectors. An employee who refused to take a polygraph test could be disciplined or even fired.

The facts:

The Administration has taken the position that employees with civil service protection could not

be fired or demoted for refusing to take a polygraph test. However, where these employees deal with highly classified information, they could be moved to less sensitive positions at the same salary level. CIA and NSA have used polygraph examinations as part of their security program for many years. Consideration has been given to expanding use of the polygraph to a small number of additional jobs that are of exceptional interest to hostile intelligence services. This is primarily a counter-espionage program rather than an anti-leak measure.

* * *

Rowan says: The congressional Office of Technology (OTA) says that "there is no scientific evidence to support the use of lie detectors for screening large numbers of people, as in an investigation for leaks"

The facts: Although the OTA study found no scientific evidence of polygraph validity for large-scale screening, it did not apply this conclusion generally to leak investigations. The OTA did find scientific evidence of polygraph validity in criminal investigations. In fact, OTA concluded: "[T]o the extent polygraph use in unauthorized disclosure investigations is similar to the way the polygraph is used in criminal investigations, there is at least some although far from conclusive scientific basis for polygraph validity."

* * *

Conclusions

Rowan says: President Reagan, because of "his oft-stated fear of Communism," is attempting to impose security restrictions that "will in fact make America more and more like Communist regimes he so abhors."

The facts: ~~This is wrong.~~ Nothing the President has proposed will change the fact that this is the most open society, with the freest press, in the world. Many ^{other} perfectly democratic countries--such

as Britain and Sweden--have much stricter official secrecy laws than the United States. Too much secrecy is obviously bad, but when it comes to intelligence and military matters, some secrecy is necessary and indeed vital to our ability to live in peace and freedom.

* * *

Rowan says: Even though President Reagan has held up on implementing the most controversial provisions of NSDD-84, Congress should refuse to compromise on these issues. Indeed, the Directive should be completely withdrawn.

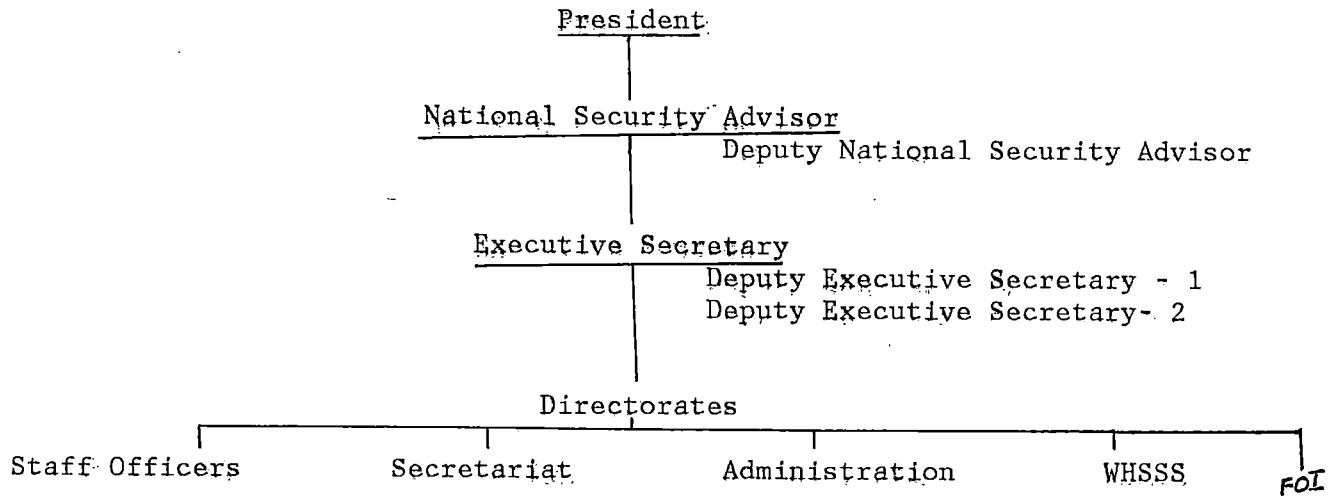
The facts: Most of the Directive's provisions have nothing to do with prepublication review or polygraphs, and have not been criticized by Congress. Rowan has articulated no reason ~~in the world~~ to withdraw these non-controversial provisions of the Directive.

From: NSMDC --CPUA
To: NSMDC --CPUA -UNCLASSIFIED-

Date and time 04/20/88 16:45:23

NOTE FROM: Maria D. Clark
SUBJECT:

ORGANIZATION OF NATIONAL SECURITY COUNCIL
(1988)



Paper Flow:

Directorates - NSC/S - WWD - DepExSec - ExSec - DAPNSA - APNSA - President