

FOIA MARKER

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

Folder Title:

Personnel Security [7]

Staff Office-Individual:

Legal Advisor-Derosa, Mary

Original OA/ID Number:

4058

Row:	Section:	Shelf:	Position:	Stack:
39	6	9	1	v

Withdrawal/Redaction Sheet

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
--------------------------	---------------	------	-------------

001. email	Home Phone. [partial] (1 page)	09/29/1995	P6/b(6)
------------	--------------------------------	------------	---------

COLLECTION:

Clinton Presidential Records
National Security Council
Legal Advisor (Mary DeRosa)
OA/Box Number: 4058

FOLDER TITLE:

Personnel Security [7]

2006-1066-F

vz876

RESTRICTION CODES

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

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

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

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

UNCLASSIFIED
NSC/RMO PROFILE

RECORD ID: 9506793
RECEIVED: 13 SEP 95 16

TO: LAKE

FROM: DAMUS, R

DOC DATE: 08 AUG 95
SOURCE REF:

KEYWORDS: INTELLIGENCE
EO

CLASSIFICATION

JD

PERSONS:

SUBJECT: PROPOSED EXECUTIVE ORDER ENTITLED CLASSIFIED NATIONAL SECURITY
INFO

1
12
11
6
12
11
6
12
11
6

ACTION: PREPARE MEMO FOR LAKE

DUE DATE: 16 SEP 95 STATUS: S

STAFF OFFICER: NONE

LOGREF:

FILES: WH

NSCP:

CODES:

D O C U M E N T D I S T R I B U T I O N

FOR ACTION
APPEL

FOR CONCURRENCE
BEERS
LEARY

FOR INFO
~~KRECKO~~

COMMENTS: _____

DISPATCHED BY _____ DATE _____ BY HAND W/ATTCH

OPENED BY: NSMEC

CLOSED BY:

DOC 1 OF 1

UNCLASSIFIED



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 8, 1995

GENERAL COUNSEL

*from Jack
Lew
Pm 379
6793*

MEMORANDUM FOR DESIGNATED AGENCY HEADS
(SEE ATTACHED DISTRIBUTION LIST)

FROM: Robert G. Damus *RGD*
General Counsel

SUBJECT: Proposed Executive Order Entitled "Classified
National Security Information"

Attached is a proposed Executive order entitled "Classified National Security Information."

It was prepared by the Information Security Oversight Office, in accordance with the provisions of Executive Order No. 11030, as amended.

On behalf of the Director of the Office of Management and Budget, I would appreciate receiving any comments you may have concerning this proposal. If you have any comments or objections, they should be received no later than Tuesday, August 15, 1995. Please be advised that agencies that do not respond by the August 15, 1995 deadline will be recorded as not objecting to the proposal.

Comments or inquiries may be submitted by telephone to Steve Aitken at 395-4728 or Bess Weaver at 395-3556 or faxed to 395-7294.

Thank you.

Attachments - Distribution List
Proposed Executive Order

cc: Jack Lew
John Koskinen
Gordon Adams
T.J. Glauthier
Bob Litan
Joe Minarik
Ken Apfel
Nancy-Ann Min
Sally Katzen
Steve Kelman
Chantale Wong

DISTRIBUTION LIST

Honorable Warren Christopher
Secretary
Department of State

Honorable William Perry
Secretary
Department of Defense

Honorable Robert E. Rubin
Secretary
Department of the Treasury

Honorable Janet Reno
United States Attorney General

Honorable Ron Brown
Secretary
Department of Commerce

Honorable Federico Pena
Secretary
Department of Transportation

Honorable Daniel S. Goldin
Administrator
National Aeronautics and Space Administration

Honorable John D. Holum
Director
Arms Control and Disarmament Agency

Honorable J. Brian Atwood
Administrator
Agency for International Development

Honorable Joseph D. Duffey
Director
United States Information Agency

Honorable Togo D. West, Jr.
Secretary
Department of the Army

Honorable John H. Dalton
Secretary
Department of the Navy

Honorable Sheila E. Widnall
Secretary
Department of the Air Force

Honorable Hazel O. O'Leary
Secretary
Department of Energy

Honorable Shirley Ann Johnson
Chairwoman
Nuclear Regulatory Commission

Honorable Robert M. Gates
Director
Central Intelligence Agency

Honorable James L. Witt
Director
Federal Emergency Management Agency

Honorable Michael Kantor
United States Trade Representative

Honorable John Gibbons
Assistant to the President
~~for Science and Technology Policy~~

Honorable Laura D. Tyson
Chair
Council of Economic Advisors

Honorable Kenneth D. Brody
President and Chairman of the Board
Export-Import Bank of the United States

Honorable Roger W. Johnson
Administrator
General Services Administration

Honorable Lee Brown
Director
Office of National Drug Control Policy

Honorable Warren Rudman
Vice Chairman
Foreign Intelligence Advisory Board

Honorable Ruth R. Harkin
Overseas Private Investment Corporation

Honorable Leon Panetta
Chief of Staff to the President

Shylife

Honorable Abner Mikva
Counsel to the President

Honorable Jack Quinn
Chief of Staff to the Vice President

Honorable John Podesta
Assistant to the President
and Staff Secretary

Honorable Anthony Lake
Assistant to the President
for National Security Affairs

456-3221

DRAFT

April 21, 1995

Order of (Date)

Classified National Security Information

Pursuant to the provisions of Section 1.4 of Executive Order No. 12,958 of April 17, 1995, entitled "Classified National Security Information," I hereby designate the following officials to classify information originally as "Top Secret", "Secret", or "Confidential":

TOP SECRET

EXECUTIVE OFFICE OF THE PRESIDENT:

The Vice President

The Chief of Staff

The Director, Office of Management and Budget

The Assistant to the President for National Security Affairs

The Director, Office of National Drug Control Policy

The Chairman, The President's Foreign Intelligence Advisory Board

The Secretary of State

The Secretary of the Treasury

The Secretary of Defense

The Secretary of the Army

The Secretary of the Navy

The Secretary of the Air Force

The Attorney General

The Secretary of Energy

The Chairman, Nuclear Regulatory Commission

The Director of Central Intelligence

The Director, Federal Emergency Management Agency

SECRET

EXECUTIVE OFFICE OF THE PRESIDENT:

The United States Trade Representative

The Director, Office of Science and Technology Policy

The Secretary of Commerce

The Secretary of Transportation

The Administrator, National Aeronautics and Space Administration

The Director, United States Arms Control and Disarmament Agency

The Administrator, Agency for International Development

The Director, United States Information Agency

DRAFT

April 21, 1995

CONFIDENTIAL

EXECUTIVE OFFICE OF THE PRESIDENT:

The Chairman, Council of Economic Advisers

The President, Export-Import Bank of the United States

The President, Overseas Private Investment Corporation

Any delegation of this authority shall be in accordance with Section 1.4(c) of the Order.

This Order shall be published in the Federal Register.

THE WHITE HOUSE

(Date)

**INFORMATION SECURITY OVERSIGHT OFFICE:
RECOMMENDATIONS FOR CHANGES TO THE
LIST OF ORIGINAL CLASSIFICATION AUTHORITIES**

<u>POSITION</u>	<u>ACTION</u>	<u>RATIONALE</u>
1. Counsellor to the President	Remove from list of authorized classifiers.	Position as formerly constituted no longer exists.
2. Deputy Chief of Staff	Remove from list of authorized classifiers.	Duties of position have been changed to minimize involvement in national security issues. Also, the Chief of Staff could serve as the original classification authority if classification action is necessary.
3. U.S. Trade Representative	Lower authorization from Top Secret to Secret	USTR has not classified at the Top Secret level for at least the past three years and the recommended action is consistent with movement in classification policy.
4. Director, Ofc. of Science and Tech. Policy	Lower authorization from Top Secret to Secret	OSTP has not classified at the Top Secret level for at least the past three years and the recommended action is consistent with movement in classification policy.
5. Director, Ofc. of Nat'l Drug Control Policy	Include on list of EOP Top Secret authorities	This position was authorized to classify at the Top Secret level after the office was created.
6. Chairman, President's Intel. Oversight Board	Remove from list of authorized classifiers.	This position no longer exists since PIOB and PFIAB were combined into one office.
7. Director, U.S. Arms Control & Disarm. Agency	Lower authorization from Top Secret to Secret	ACDA has not classified at the Top Secret level for at least the past two years and the recommended action is consistent with movement in classification policy.

<u>POSITION</u>	<u>ACTION</u>	<u>RATIONALE</u>
8. Administrator, Nat'l Aeronautics and Space Administration	Lower authorization from Top Secret to Secret.	NASA has not classified at the Top Secret level for at least the past three years and the recommended action is consistent with movement in classification policy. Also, NASA's involvement in classified activities has dropped markedly.
9. Administrator of Gen'l Services	Remove from list of authorized classifiers.	GSA's authority was based solely on a further delegation to the Director of ISOO, who is no longer in GSA.
10. Chairman, Council of Econ. Advisers	Lower authorization from Secret to Confidential.	CEA's minimal use of original classification authority has been limited to an action or two at the Confidential level.
11. President's Personal Representative for Micronesian Status Negotiations	Remove from list of authorized classifiers.	Position no longer exists independent of the Department of State.
12. Administrator, Environmental Protection Agency	Remove from list of authorized classifiers.	EPA was added to the list of original classifying agencies at the insistence of an Administrator of many years ago. In recent years, EPA has had no opportunity or need to classify originally. Should such an occasion occur in international negotiations, the State Department can serve as the original classification authority.

Presidential Documents

11, 1982

Order of May 7, 1982

National Security Information

Pursuant to the provisions of Section 1.2 of Executive Order No. 12356 of April 2, 1982, entitled "National Security Information," I hereby designate the following officials to classify information originally as "Top Secret", "Secret", or "Confidential":

TOP SECRET**EXECUTIVE OFFICE OF THE PRESIDENT:**

The Vice President
The Counsellor to the President
The Chief of Staff and Assistant to the President
The Deputy Chief of Staff and Assistant to the President
The Director, Office of Management and Budget
The United States Trade Representative
The Assistant to the President for National Security Affairs
The Director, Office of Science and Technology Policy
The Chairman, The President's Foreign Intelligence Advisory Board
The Chairman, The President's Intelligence Oversight Board

The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Secretary of the Army
The Secretary of the Navy
The Secretary of the Air Force
The Attorney General
The Secretary of Energy
The Chairman, Nuclear Regulatory Commission
The Director, United States Arms Control and Disarmament Agency
The Director of Central Intelligence
The Administrator, National Aeronautics and Space Administration
The Administrator of General Services
The Director, Federal Emergency Management Agency

SECRET**EXECUTIVE OFFICE OF THE PRESIDENT:**

The Chairman, Council of Economic Advisers
The President's Personal Representative for Micronesian Status Negotiations

The Secretary of Commerce

The Secretary of Transportation

The Administrator, Agency for International Development

The Director, International Communication Agency

CONFIDENTIAL

The President, Export-Import Bank of the United States

The President, Overseas Private Investment Corporation

The Administrator, Environmental Protection Agency

Any delegation of this authority shall be in accordance with Section 12(d) of the Order.

This Order shall be published in the Federal Register.

Ronald Reagan

THE WHITE HOUSE

May 7, 1982

cc
E-7-82 pen
g code 01-M

ACTION

MEMORANDUM FOR ANTHONY LAKE

THROUGH: R. RAND BEERS

FROM: EDWARD J. APPEL

SUBJECT: Implementing Directive for Executive Order 12958,
"Classified National Security Information"

Executive Order 12958 (Classified Information) directs OMB, through ISOO, to issue implementing directives binding on all agencies in four specified areas. The directives are to be issued in consultation with you and with the Co-Chairs of the Security Policy Board (SPB). ISOO's draft guidelines were forwarded after interagency coordination September 19, 1995 and final interagency approval at a meeting of the Security Policy Forum on September 29, 1995. The SPB Co-Chairs' concurrence is pending and expected soon. OMB asked for our prompt response, so that the guidelines can be printed in the Federal Register and become effective October 14, 1995.

A review of the guidelines shows that they are complete, sufficient, clear and meet the requirements of the EO. However, as originally drafted, foreign government information might have been declassified without consulting with the foreign government involved. As you may be aware, our Australian allies (through a meeting with Sandy Berger), British and other close allies have expressed strong concerns about both the EO and draft guidelines. Australian Ambassador Donald Russell and Graham Kearns, Defense Policy Counselor, expressed a need to strengthen the guidelines in discussions with both the NSC and ISOO. Language which satisfies their concerns (which they have seen and approved) has been substituted, in coordination with ISOO, SPB staff and concerned departments.

Changes to the draft guidelines during the September 29th Forum meeting settled all agencies' specific concerns. State (through Amb. Anthony Quainton) had written to you September 19, 1995. State's concerns now have all been addressed in revisions to the draft.

The attached letter to OMB through ISOO accepts the revisions made to date and asks for coordination with NSC staff of the final draft.

Attached at Tab I for your signature is a memorandum for OMB, attention Information Security Oversight Office (ISOO) and at Tab II a letter dated September 19, 1995 from OMB with draft guidelines implementing EO 12958. At Tab IIA is draft language provided by ISOO.

Concurrence by: Alan Kreczko William Leary

RECOMMENDATION:

That you sign the letter to OMB through ISOO at Tab I.

Attachments

Tab I Memorandum to OMB through ISOO
Tab II Incoming correspondence from OMB
Tab A ISOO fax dtd 9/29 transmitting revised foreign government
 information

MEMORANDUM FOR ALICE M. RIVLIN
DIRECTOR
OFFICE OF MANAGEMENT AND BUDGET

ATTENTION:
STEVEN GARFINKEL, DIRECTOR
INFORMATION SECURITY OVERSIGHT OFFICE

SUBJECT: Implementing Directive for
 Executive Order 12958, "Classified
 National Security Information"

Thank you for the opportunity to review the draft guidelines transmitted with your September 19, 1995 letter.

Review of the draft Implementing Directive for Executive Order 12958 showed it to be an excellent document.

I understand that the Security Policy Forum considered changes and voted to accept the document as drafted, with minor changes, on September 29, 1995. One particular concern of the NSC was the declassification of foreign government information. As you know, the Australians and some others have voiced concern that the Guidelines' language include consultation with the foreign country concerned, prior to declassification. Based on discussions between Edward J. Appel of the Intelligence Programs Office at NSC and Steven Garfinkel, I am told that language satisfactory to the Australians was agreed to, and that Defense Department has concurred.

The final, pre-publication draft of the Guidelines should be provided for consultation to the NSC Staff through Mr. Appel. Thank you for your work on this important project.

Anthony Lake
Assistant to the President
for National Security Affairs

Baker, James E.

From: Kreczko, Alan J.
To: Baker, James E.
Cc: /R, Record at A1
Subject: FW: EO 12958 [UNCLASSIFIED]
Date: Thursday, September 28, 1995 10:30AM

fyi

From: Leary, William H.
To: Appel, Edward J.; Kreczko, Alan J.
CC: /R, Record at A1
Subject: RE: EO 12958 [UNCLASSIFIED]
Date: Thursday, September 28, 1995 08:21 AM

Ed,

I like Alan's suggestion for reformulating the "should"/"shall" conundrum; it's along the lines of our discussion yesterday. What do you think?

From: Kreczko, Alan J.
To: Appel, Edward J.; Leary, William H.
CC: /R, Record at A1
Subject: RE: EO 12958 [UNCLASSIFIED]
Date: Wednesday, September 27, 1995 09:28 PM

Ed/Bill,

1. I would like to hear what examples Steve Garfinkel has in mind before giving a view on whether it should be "should" or "shall". Would another possibility be to say "shall consult the foreign government unless the State Department determines such consultation is not necessary?"
2. If I understand point 2 on page 2 of the ISOO draft, I have a problem with it. I read that paragraph as saying that if you pick a date for declassification, and that date passes, the information is automatically declassified. Shouldn't that be is presumptively declassified? Let's say I pick the year 2000 for declassification, based on my best guess of what foreign policy implications will be for release at that time. The year 2000 comes around, and I forget to review for extension. However, foreign affairs situation at that point is different from what I anticipated, and release of the document would cause serious foreign affairs problems. Is the document irrevocably declassified because I did not extend? Shouldn't it nonetheless be reviewed before it is released to see if really should be declassified? Otherwise, it would seem that the incentive is always to classify for maximum period permitted.
3. Can there be some exception to the requirement to provide all of that information when classifying a document -- see pages 7 - 12 -- at least for informal communications like E-mail?

From: Leary, William H.
To: Appel, Edward J.
CC: /R, Record at A1; Kreczko, Alan J.
Subject: EO 12958 [UNCLASSIFIED]
Date: Wednesday, September 27, 1995 04:22 PM

Ed,

I have a few comments on your memo to Tony recommending changes in the Implementing Directive for EO 12958 regarding "foreign government information:"

1. I annotated your draft with a few editorial changes.
2. Your revised Section 2001.12(c), 3rd line from bottom: "classifying" should be "declassifying"

3. I would strike all your bolded new language suggested for 2001.12(c) because those higher standards for continuing classification in 3.4 apply only to records subject to automatic declassification, i.e., archival records that are 25 years old. If it is a 5-year old record being reviewed for declassification, e.g., a lower set of standards ((1.6(d)) will satisfy the requirement for continued classification.

4. Most seriously, I do not concur in your recommendation, in all three sections discussing foreign government information, to substitute the word : "shall" for "should" -- for the following reasons:

1. There are rare occasions when the United States government should have the discretion to make a decision without formally consulting. Steve Garfinkel can cite specific examples.

2. According to Steve, the Australian officials who complained about the original draft language on this issue say they would be satisfied if we strike the word "ordinarily" in each of these sections.

Withdrawal/Redaction Marker

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. email	Home Phone. [partial] (1 page)	09/29/1995	P6/b(6)

COLLECTION:

Clinton Presidential Records
National Security Council
Legal Advisor (Mary DeRosa)
OA/Box Number: 4058

FOLDER TITLE:

Personnel Security [7]

2006-1066-F

vz876

RESTRICTION CODES

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

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

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

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

Baker, James E.

From: Leary, William H.
To: Appel, Edward J.
Cc: /R, Record at A1; Baker, James E.; Kreczko, Alan J.
Subject: EO 12958 (UNCLASSIFIED)
Date: Friday, September 29, 1995 12:14PM

Ed,

I have a few more comments on the implementing directive, listed below. Alan and I also think it would be appropriate to include in your memo to Tony on this matter a reference to the letter to Tony from Quainton at State. On the latter, you should say something like the following:

Anthony Quainton, Assistant Secretary of State for Diplomatic Security, wrote to you on September 19 suggesting changes to sections of the implementing directive that deal with "foreign government information," classification challenges, and the meaning of "jurisdiction over information." We believe that each of these concerns has been addressed by recent changes to the draft directive. I suggest that you authorize me (or Bill Leary) to convey this information to Mr. Quainton.

Additional comments:

2001.11(b). Shouldn't such requests also be forwarded through the APNSA, consistent with sections 5.2 and 5.3 of the Order.

2001.12(a)(2). I strongly endorse Alan's comments in his earlier e-mail to the effect that automatic declassification will encourage classifiers to exempt a lot of records from the 10 year rule. If they do, that means -- also automatically -- that a document is classified for 25 years, according to ISOO.

E-mail. This probably is not a subject that can be successfully addressed in this document. However, Alan is absolutely right in suggesting that a literal application of the marking requirements of this directive to e-mail will seriously impair its usefulness. It definitely is an issue that will require some study and a lot of flexibility. More generally, the marking and portion marking requirements are so burdensome that I will be very surprised if there is not some backlash.

I will be off this afternoon. I should be home by 5:30 P6/(b)(6) I put a copy of the Quainton letter in your box.

[001]



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 19, 1995

MEMORANDUM FOR ANTHONY LAKE
ASSISTANT TO THE PRESIDENT
FOR NATIONAL SECURITY AFFAIRS

FROM: Alice M. Rivlin 
SUBJECT: Implementing Directive for
Executive Order 12958, "Classified
National Security Information"

In accordance with section 5.2 of Executive Order No. 12958, "Classified National Security Information," I attach for your review and comment a draft directive on those provisions of the Order for which the Director of the Office of Management and Budget is responsible for implementation. The Information Security Oversight Office has prepared this draft with the assistance and review of representatives of the agencies most involved with classified information. This draft incorporates many of the suggestions that the agencies have offered. Representatives of these agencies have also been made aware of the substance of the draft.

In order that I can meet the Order's requirement for issuance of the directive, please submit your comments and suggestions to OMB, to the attention of the Information Security Oversight Office, no later than October 2, 1995.

Attachment

PART 2001—Classified National Security Information

Subpart A—Classification

Sec.

- 2001.10 Classification standards [1.2]
- 2001.11 Classification authority [1.4]
- 2001.12 Duration of classification [1.6]
- 2001.13 Classification challenges [1.9]
- 2001.14 Classification guides [2.3]

Subpart B—Identification and Markings

- 2001.20 General [1.7]
- 2001.21 Original classification [1.7(a)]
- 2001.22 Derivative classification [2.2]
- 2001.23 Additional requirements [1.7]
- 2001.24 Declassification markings [Reserved]

Subpart C—Self-Inspections

- 2001.30 General [5.6]
- 2001.31 Coverage [5.6(c)(4)]

Subpart D—Security Education and Training

- 2001.40 General [5.6]
- 2001.41 Coverage [5.6(c)(3)]

Subpart E—Declassification

- 2001.50 Definitions [3.1]
- 2001.51 Automatic declassification [3.4]
- 2001.52 Systematic declassification review [3.5]
- 2001.53 Declassification guides [3.5(b)]
- 2001.54 Mandatory review for declassification [3.6, 3.7]

Subpart F—Reporting

- 2001.60 Statistical reporting [5.3]
- 2001.61 Accounting for costs [5.6]
- 2001.62 Publication and effective date [6.2]

Subpart A—Classification

§2001.10 Classification standards [Sec. 1.2(a)]*

Section 1.2(a) of the Order sets forth the conditions for classifying information in the first instance. One of these conditions, the ability to identify or describe the damage to the national security, is critical to the process of making an original classification decision. There is no requirement, at the time of the decision, for the original classification authority to prepare a written description of such damage. However, the original classification authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand.

§2001.11 Classification authority [1.4]

(a) *General.* Agencies with original classification authority shall establish a training program for original classifiers in accordance with Subpart D, below.

(b) *Requests for original classification authority.* Agencies not possessing such authority shall forward requests to the Director of the Information Security Oversight Office (ISOO). The agency head must make the request and shall provide a specific justification of the need for this authority. The Director of ISOO shall forward the request, along with the Director's recommendation, to the President through the Director of the Office of Management and Budget (OMB) within 30 days. Agencies wishing to increase their assigned level of original classification authority shall forward requests in accordance with the above procedures.

§2001.12 Duration of classification [1.6]

(a) *Determining duration of classification for information originally classified under the Order.*

(1) *Establishing duration of classification.* When determining the duration of classification for information originally classified under this Order, an original classification authority shall follow the sequence listed in paragraphs (A), (B), and (C), below.

* Bracketed references pertain to related sections of Executive Order 12958.

(A) The original classification authority shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's sensitivity, and shall assign such date or event as the declassification instruction.

(B) If unable to determine a date or event of less than 10 years, the original classification authority shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

(C) The original classification authority may assign an exemption designation to the information only if the information qualifies for exemption from automatic declassification as described in section 1.6(d) of the Order.

(2) *Extending duration of classification for information originally classified under this Order.* Extensions of classification are not automatic. If an original classification authority with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event. If an original classification authority has assigned a date or event for declassification that is 10 years or less from the date of classification, an original classification authority with jurisdiction over the information may extend the classification duration of such information for additional periods not to exceed 10 years at a time.

(A) For information in records determined to have permanent historical value, successive extensions may not exceed a total of 25 years from the date of the information's origin. Continued classification of this information beyond 25 years is governed by section 3.4 of the Order.

(B) For information in records not determined to have permanent historical value, successive extensions may exceed 25 years from the date of the information's origin.

(3) *Conditions for extending classification.* When extending the duration of classification, the original classification authority must:

(A) be an original classification authority with jurisdiction over the information;

(B) ensure that the information continues to meet the standards for classification under the Order; and

(C) make reasonable attempts to notify all known holders of the information.

(b) *Information classified under prior orders.*

(1) *Specific date or event.* Unless declassified earlier, information marked with a specific date or event for declassification under a prior order is automatically declassified upon that date or event. However, if the information is contained in records determined by the Archivist of the United States to be permanently valuable, and the prescribed date or event will take place more than 25 years from the information's origin, the declassification of the information will instead be subject to section 3.4 of the Order.

(2) *Indefinite duration of classification.* For information marked "Originating Agency's Determination Required," its acronym "OADR," or with some other marking indicating an indefinite duration of classification under a prior order:

(A) an authorized declassification authority with jurisdiction over the information may declassify it;

(B) an authorized original classification authority with jurisdiction over the information may specify a date or event for declassification; or

(C) unless declassified earlier, such information contained in records determined by the Archivist of the United States to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to section 3.4 of the Order.

(c) *Foreign government information.* When foreign government information is being considered for declassification or appears to be subject to automatic declassification, ordinarily the declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

§2001.13 Classification challenges [1.9]

(a) *Challenging classification.* Authorized holders wishing to challenge the classification status of information shall present such challenges to an original classification authority with jurisdiction over the information. An authorized holder is any individual, including an individual external to the agency, who has been granted access to specific classified information in

accordance with section 4.2(g) of the Order. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified, or is classified at a certain level.

(b) *Agency procedures.*

(1) Because the Order encourages authorized holders to challenge classification as a means for promoting proper and thoughtful classification actions, agencies shall ensure that no retribution is taken against any authorized holders bringing such a challenge in good faith.

(2) Agencies shall establish a system for processing, tracking and recording formal classification challenges made by authorized holders. Records of challenges shall be subject to oversight by the Interagency Security Classification Appeals Panel. Agencies shall consider classification challenges separately from Freedom of Information Act or other access requests, and shall establish a system of processing challenges that does not place classification challenges in the same processing system as these access requests.

(3) Agencies shall ensure that each challenge is reviewed by an original classification authority with jurisdiction over the challenged information. If the challenger is not satisfied with the decision, the challenger may request a review by an impartial official or panel of the originating agency. The agency shall provide an initial written response to a challenge within 60 days. If the agency is unable to respond to the challenge within 60 days, the agency must acknowledge the challenge in writing, and provide a date by which the agency will respond. The acknowledgment must include a statement that if no agency response is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel for a decision. The challenger may also forward the challenge to the Interagency Security Classification Appeals Panel if an agency has not responded to an internal appeal within 90 days of the agency's receipt of the appeal.

(4) Agency responses to those challenges it denies shall include, at a minimum: (1) A concise reason for denial of the challenge, unless such reason would reveal additional classified information; (2) the name(s) or title(s) of the official(s) reviewing the challenge; and (3) the challenger's appeal rights, including procedures for forwarding the appeal to the Interagency Security Classification Appeals Panel.

(5) Whenever an agency receives a classification challenge to information that has been the subject of a challenge within the past two years, or that is the subject of pending litigation, the agency is not required to process the challenge beyond informing the challenger of this fact and of the challenger's appeal rights, if any.

(c) *Additional considerations.*

(1) Challengers and agencies shall attempt to keep all challenges, appeals and responses unclassified. However, classified information contained in a challenge, an agency response, or an appeal shall be handled and protected in accordance with the Order and its implementing directives. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it.

(2) The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries should be encouraged as a means of holding down the number of formal challenges.

§2001.14 Classification guides [2.3]

(a) *Preparation of classification guides.* Originators of classification guides are encouraged to consult users of guides for input when developing or updating guides. When possible, originators of classification guides are encouraged to communicate within their agencies and with other agencies that are developing guidelines for similar activities to ensure the consistency and uniformity of classification decisions. Each agency shall maintain a list of its classification guides in use.

(b) *General content of classification guides.* Classification guides shall, at a minimum:

- (1) identify the subject matter of the classification guide;
- (2) identify the original classification authority by name or personal identifier, and position;
- (3) identify an agency point-of-contact or points-of-contact for questions regarding the classification guide;
- (4) provide the date of issuance or last review;

- (5) state precisely the elements of information to be protected;
 - (6) state which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified;
 - (7) state, when applicable, special handling caveats;
 - (8) prescribe declassification instructions or the exemption category from automatic declassification for each element of information. When reviewing or updating a guide, the duration of classification prescribed for each element of information shall be calculated from the date of the information's origin. Also, when citing the exemption category listed in section 1.6(d)(8) of the Order, the guide shall also specify the applicable statute, treaty or international agreement; and
 - (9) state a concise reason for classification which, at a minimum, cites the applicable classification category or categories in section 1.5 of the Order.
- (c) *Dissemination of classification guides.* Classification guides shall be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information.
- (d) *Requirement for review of classification guides.* Originators of classification guides are encouraged to consult the users of guides for input when reviewing or updating guides. Also, users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide. Classification guides shall be reviewed and updated as circumstances require, but, in any event, at least once every five years.

Subpart B—Identification and Markings

§2001.20 General [1.7]

A uniform security classification system requires that standard markings be applied to classified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of classified information created after October 14, 1995, shall not deviate from the following prescribed formats. If markings cannot be affixed to specific classified information or materials, the originator shall provide holders or recipients of the information with written instructions for protecting the information.

Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

§2001.21 Original classification [1.7(a)]

E-mail?

(a) *Primary markings.* On the face of each originally classified document, the classifier shall apply the following markings.

(1) *Classification authority.* The name or personal identifier, and position title of the original classifier shall appear on the "Classified By" line. An example might appear as:

Classified By: David Smith, Chief, Division 5
or

Classified By: ID#IMNO1, Chief, Division 5

(2) *Agency and office of origin.* If not otherwise evident, the agency and office of origin shall be identified and placed below the name on the "Classified By" line. An example might appear as:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of
Administration

(3) *Reason for classification.* The original classifier shall identify the reason(s) for the decision to classify. The classifier shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.5 plus the letter(s) that corresponds to that classification category in section 1.5 of the Order.

(A) These categories, as they appear in the Order, include:

- "(a) military plans, weapons, or operations;
- (b) foreign government information;
- (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security."

(B) An example might appear as follows:

Classified By: David Smith, Chief, Division 5
Department of Good Works,
Office of Administration
Reason: **Vulnerabilities or capabilities of plans
relating to the national security**
or
Reason: **1.5(g)**

(C) When the reason for classification is not apparent from the content of the information, e.g., classification by compilation, the classifier shall provide a more detailed explanation of the reason for classification.

(4) *Declassification instructions.* The duration of the original classification decision shall be placed on the "Declassify On" line. The classifier will apply one of the following instructions.

(A) The classifier will apply a date or event for declassification that corresponds to the lapse of the information's national security sensitivity, which may not exceed 10 years from the date of the original decision. When linking the duration of classification to a specific date or event, mark that date or event as follows:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of
Administration
Reason: 1.5(g)
Declassify On: **October 14, 2004**
or
Declassify On: **Completion of Operation**

(B) When a specific date or event is not apparent, the classifier will apply the date that is 10 years from the date of the original decision. For example, on a document that contains information classified on October 14, 1995, mark the "Declassify On" line as follows:

DRAFT

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of
Administration
Reason: 1.5(g)
Declassify On: October 14, 2005

(C) Upon the determination that the information is exempted from declassification at 10 years, the classifier will apply the letter "X" plus a brief recitation of the exemption category(ies), or the letter "X" plus the number that corresponds to that exemption category(ies) in section 1.6(d) of the Order.

- X1: "reveal an intelligence source, method, or activity, or a cryptologic system or activity;"
- X2: "reveal information that would assist in the development or use of weapons of mass destruction;"
- X3: "reveal information that would impair the development or use of technology within a United States weapons system;"
- X4: "reveal United States military plans, or national security emergency preparedness plans;"
- X5: "reveal foreign government information;"
- X6: "damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;"
- X7: "impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or"
- X8: "violate a statute, treaty, or international agreement."

For example, a document containing information exempted from automatic declassification may appear as follows:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of
Administration
Reason: 1.5(g)
Declassify On: X-U.S. military plans
or
Declassify On: X4

(b) *Overall marking.* The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the informational text.

(1) Conspicuously place the overall classification 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) For documents containing information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked "Secret" and other information marked "Confidential," the overall marking would be "Secret."

(3) Each interior page of a classified document shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation "Unclassified" when it is applicable, or with the highest overall classification of the document.

(c) *Portion marking.* Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics and the like, shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding or following the portion to which it applies.

(1) To indicate the appropriate classification level, the symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used.

(2) An agency head or senior agency official may request a waiver from the portion marking requirement for a specific category of information. Such a request shall be submitted to the Director of ISOO and should include the reasons that the benefits of portion marking are outweighed by other factors. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver.

(d) *Classification extensions.*

(1) An original classification authority may extend the duration of classification for successive periods not to exceed 10 years at a time. For information contained in records determined to be permanently valuable, multiple extensions shall not exceed 25 years from the date of the information's origin.

(2) The "Declassify On" line shall be revised to include the new declassification instructions, and shall include the identity of the person authorizing the extension and the date of the action.

(3) The office of origin shall make reasonable attempts to notify all holders of such information. Classification guides shall be updated to reflect such revisions.

(4) An example of an extended duration of classification may appear as follows:

Classified By:	David Smith, Chief, Division 5 Department of Good Works, Office of Administration
Reason:	1.5(g)
Declassify On:	Classification extended on December 1, 2000 until December 1, 2010, by David Jones, Chief, Division 5

(e) Marking information exempted from automatic declassification at 25 years.

(1) When an agency head or senior agency official exempts permanently valuable information from automatic declassification at 25 years, the "Declassify On" line shall be revised to include the symbol "25X" plus a brief reference to the pertinent exemption category(ies) or the number(s) that corresponds to that category(ies) in section 3.4(b) of the Order. Other than when the exemption pertains to the identity of a confidential human source, or a human intelligence source, the revised "Declassify On" line shall also include the new date or event for declassification.

(2) The pertinent exemptions, using the language of section 3.4(b) of the Order, are the following:

25X1: "reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;"

- 25X2: "reveal information that would assist in the development or use of weapons of mass destruction;"
- 25X3: "reveal information that would impair U.S. cryptologic systems or activities;"
- 25X4: "reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;"
- 25X5: "reveal actual U.S. military war plans that remain in effect;"
- 25X6: "reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;"
- 25X7: "reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;"
- 25X8: "reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or"
- 25X9: "violate a statute, treaty, or international agreement."

(3) The pertinent portion of the marking would appear as follows:

Declassify On:	25X-State-of-the-art technology within U.S. weapon system October 1, 2010 or
Declassify On:	25X4 October 1, 2010

(4) Documents should not be marked with a "25X" marking until the agency has been informed that the President or the Interagency Security Classification Appeals Panel concurs with the proposed exemption.

(5) Agencies need not apply a "25X" marking to individual documents contained in a file series exempted from automatic declassification under section 3.4(c) of the Order until the individual document is removed from the file.

§2001.22 Derivative classification [2.2]

(a) *General.* Information classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in §2001.20 and §2001.21, above, except as provided below. Information for

these markings shall be carried forward from the source document or taken from instructions in the appropriate classification guide.

(b) *Source of derivative classification.*

(1) The derivative classifier shall concisely identify the source document or the classification guide on the "Derived From" line, including the agency and office of origin, and the date of the source or guide. An example might appear as follows:

Derived From: Memo
"Funding Problems," October 20, 1995
Ofc. of Admin., Department of Good Works
or
Derived From: CG No. 1, Department of Good
Works, dated October 20, 1995

(2) When a document is classified derivatively on the basis of more than one source document or classification guide, the "Derived From" line shall appear as follows:

Derived From: Multiple Sources

The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. When practicable, this list should be included in or with all copies of the derivatively classified document.

(3) A document derivatively classified on the basis of a source document that is itself marked "Multiple Sources" shall cite the source document on its "Derived From" line rather than the term "Multiple Sources." An example might appear as follows:

Derived From: Report entitled, "New Weapons,"
dated October 20, 1995,
Department of Good Works,
Office of Administration

(c) *Reason for classification.* The reason for the original classification decision, as reflected in the source document(s) or classification guide, is not required to be transferred in a derivative classification action. If included, however, it shall conform to the standards in §2001.21(a)(3), above.

(d) *Declassification instructions.*

(1) The derivative classifier shall carry forward the instructions on the "Declassify On" line from the source document to the derivative document, or the duration instruction from the classification guide.

(2) When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the "Declassify On" line shall reflect the longest duration of any of its sources.

(3) When a document is classified derivatively from a source document(s) or classification guide that contains the declassification instruction, "Originating Agency's Determination Required," or "OADR," unless otherwise instructed by the original classifier, the derivative classifier shall carry forward:

(A) the fact that the source document(s) was marked with this instruction; and

(B) the date of origin of the most recent source document(s) or classification guide.

An example might appear as follows:

Declassify On: Source marked "OADR"
Date of origin: October 20, 1990

This marking will permit the determination of when the classified information is 25 years old and, if permanently valuable, subject to automatic declassification under section 3.4 of the Order.

(e) *Overall marking.* The derivative classifier shall conspicuously mark the classified document with the highest level of classification of information included in the document, as provided in §2001.21(b), above.

(f) *Portion marking.* Each portion of a derivatively classified document shall be marked in accordance with its source, and as provided in §2001.21(c), above.

§2001.23 Additional requirements [1.7]

(a) *Marking prohibitions.* Markings other than "Top Secret," "Secret," and "Confidential," such as "For Official Use Only," or "Limited Official Use," shall not be used to identify classified 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 classified national security information. The terms "Top Secret," "Secret," and "Confidential" should not be used to identify non-classified executive branch information.

(b) *Agency prescribed special markings.* Agencies shall refrain from the use of special markings when they merely restate or emphasize the principles and standards of the Order and this directive. Upon request, the senior agency official shall provide the Director of ISOO with a written explanation for the use of agency special markings.

(c) *Transmittal documents.* A transmittal document shall indicate on its face the highest classification level of any classified information attached or enclosed. The transmittal shall also include conspicuously on its face the following or similar instructions, as appropriate:

UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE REMOVED
or
UPON REMOVAL OF ATTACHMENTS, THIS DOCUMENT IS
(CLASSIFICATION LEVEL)

(d) *Foreign government information.* Documents that contain foreign government information shall include either the marking "Foreign Government Information," "FGI," or a marking that otherwise indicates that the information is of foreign origin. 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.

(e) *Working papers.* A working paper is defined as documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information shall be dated when created, marked with the highest classification of any information contained in them, protected at that level, and destroyed when no longer needed. When any of the following conditions applies, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level:

- (1) released by the originator outside the originating activity;
- (2) retained more than 180 days from the date of origin; or
- (3) filed permanently.

(f) *Other material.* Bulky material, equipment and facilities, etc., shall be clearly identified in a manner that leaves no doubt about the classification status of the material, the level of protection required, and the duration of classification. Upon a finding that identification would itself reveal classified information, such identification is not required. Supporting documentation for such a finding must be maintained in the appropriate security facility and in any applicable classification guide.

(g) *Unmarked materials.* Information contained in unmarked records or presidential or related materials and which (1) pertains to the national defense or foreign relations of the United States; and (2) has been maintained and protected as classified information under prior orders shall continue to be treated as classified information under the Order, and is subject to its provisions regarding declassification.

§2001.24 Declassification markings
[RESERVED]

Subpart C—Self-Inspections

§2001.30 General [5.6]

(a) *Purpose.* This subpart sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include the periodic review and assessment of the agency's classified product. "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under the Order.

(b) *Applicability.* These standards are binding on all executive branch agencies that create or handle classified information. Pursuant to Executive Order 12829, the National Industrial Security Program Operating Manual (NISPOM) prescribes the security requirements, restrictions and safeguards applicable to industry, including the conduct of contractor self-inspections. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958 and this directive.

(c) *Responsibility.* The senior agency official is responsible for the agency's self-inspection program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* The official(s) responsible for the program shall determine the means and methods for the conduct of self-inspections. These may include:

(1) a review of relevant security directives, guides and instructions;
(2) interviews with producers and users of classified information; (3) a review of access and control records; and (4) a review of a sample of classified documents generated by agency activities.

(e) *Frequency.* The official(s) responsible for the program shall set the frequency of self-inspections on the basis of program needs and the degree of classification activity. Activities that originate significant amounts of classified information should conduct at least one document review per year.

(f) *Reporting.* The format for documenting findings shall be set by the official(s) responsible for the program.

§2001.31 Coverage [5.6(c)(4)]

(a) *General.* These standards are not all-inclusive. Each agency may expand upon the coverage according to program and policy needs. Each self-inspection of an agency activity need not include all the elements covered below. Agencies without original classification authority need not include in their self-inspections those elements of coverage pertaining to original classification.

(b) *Elements of coverage.*

(1) *Original classification.*

(A) Evaluate original classifiers' general understanding of the process of original classification, including the:

(i) applicable standards for classification;

(ii) levels of classification and the damage criteria associated with each; and

(iii) required classification markings.

(B) Determine if delegations of original classification authority conform with the requirements of the Order, including whether:

(i) delegations are limited to the minimum required to administer the program;

(ii) designated original classifiers have a demonstrable and continuing need to exercise this authority;

(iii) delegations are in writing and identify the official by name or position title; and

(iv) new requests for delegation of classification authority are justified.

(C) Assess original classifiers' familiarity with the duration of classification requirements, including:

(i) assigning a specific date or event for declassification when possible;

(ii) establishing ordinarily a maximum 10-year duration of classification when an earlier date or event cannot be determined;

(iii) limiting extensions of classification for specific information for successive periods not to exceed 10 years at a time; and

(iv) exempting from declassification within 10 years specific information as provided in section 1.6 of the Order.

(D) Conduct a review of a sample of classified information generated by the inspected activity to determine the propriety of classification and the application of proper and full markings.

(E) Evaluate classifiers' actions to comply with the standards specified in §2001.14 and §2001.53 of this directive, relating to classification and declassification guides, respectively.

(F) Verify observance with the prohibitions on classification and limitations on reclassification.

(G) Assess whether the agency's classification challenges program meets the requirements of the Order and this directive.

(2) *Derivative classification.* Assess the general familiarity of individuals who classify derivatively with the:

- (A) conditions for derivative classification;
- (B) requirement to consult with the originator of the information when questions concerning classification arise;
- (C) proper use of classification guides; and
- (D) proper and complete application of classification markings to derivatively classified documents.

(3) *Declassification.*

- (A) Verify whether the agency has established, to the extent practical, a system of records management to facilitate public release of declassified documents.
- (B) Evaluate the status of the agency declassification program, including the requirement to:
 - (i) comply with the automatic declassification provisions regarding historically valuable records over 25 years old;
 - (ii) declassify, when possible, historically valuable records prior to accession into the National Archives;
 - (iii) provide the Archivist with adequate and current declassification guides;
 - (iv) ascertain that the agency's mandatory review program conforms to established requirements; and
 - (v) determine whether responsible agency officials are cooperating with the Archivist in the development and maintenance of a Government-wide database of information that has been declassified.

(4) *Safeguarding.*

- (A) Monitor agency adherence to established safeguarding standards.
- (B) Assess compliance with controls for access to classified information.

(C) Evaluate the effectiveness of the agency's program in detecting and processing security violations and preventing recurrences.

(D) Assess compliance with the procedures for identifying, reporting and processing unauthorized disclosures of classified information.

(E) Evaluate the effectiveness of procedures to ensure that:

(i) the originating agency exercises control over the classified information it generates;

(ii) holders of classified information do not disclose information originated by another agency without that agency's authorization; and

(iii) departing or transferred officials return all classified information in their possession to authorized agency personnel.

(5) *Security education and training.* Evaluate the effectiveness of the agency's security education and training program in familiarizing appropriate personnel with classification procedures; and determine whether the program meets the standards specified in Subpart D of this directive.

(6) *Management and oversight.*

(A) Determine whether original classifiers have received prescribed training.

(B) Verify whether the agency's special access programs:

(i) adhere to specified criteria in the creation of these programs;

(ii) are kept to a minimum;

(iii) provide for the conduct of internal oversight; and

(iv) include an annual review of each program to determine whether it continues to meet the requirements of the Order.

(C) Assess whether:

(i) senior management demonstrates commitment to the success of the program, including providing the necessary resources for effective implementation;

(ii) producers and users of classified information receive guidance with respect to security responsibilities and requirements;

(iii) controls to prevent unauthorized access to classified information are effective;

(iv) contingency plans are in place for safeguarding classified information used in or near hostile areas;

(v) the performance contract or other system used to rate civilian or military personnel includes the management of classified information as a critical element or item to be evaluated in the rating of: (1) original classifiers; (2) security managers, classification management officers and security specialists; and (3) other employees significantly involved with classified information; and

(vi) a method is in place for collecting information on the costs associated with the implementation of the Order.

Subpart D—Security Education and Training

§2001.40 General [5.6]

(a) *Purpose.* This subpart sets standards for agency security education and training programs. Implementation of these standards should: (1) ensure that all executive branch employees who create, process or handle classified information have a satisfactory knowledge and understanding about classification, safeguarding, and declassification policies and procedures; (2) increase uniformity in the conduct of agency security education and training programs; and (3) reduce improper classification, safeguarding and declassification practices.

(b) *Applicability.* These standards are binding on all executive branch departments and agencies that create or handle classified information. Pursuant to Executive Order 12829, the NISPOM prescribes the security requirements, restrictions, and safeguards applicable to industry, including the conduct of contractor security education and training. The standards

established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958 and this directive.

(c) *Responsibility.* The senior agency official is responsible for the agency's security education and training program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* Security education and training should be tailored to meet the specific needs of the agency's security program, and the specific roles employees are expected to play in that program. The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, and other media and methods.

(e) *Frequency.* The frequency of agency security education and training will vary in accordance with the needs of the agency's security classification program. Each agency shall provide some form of refresher security education and training at least annually.

§2001.41 Coverage [5.6(c)(3)]

(a) *General.* Each department or agency shall establish and maintain a formal security education and training program which provides for initial and refresher training, and termination briefings. This subpart establishes security education and training standards for original classifiers, declassification authorities, security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. These standards are not intended to be all-inclusive. The official responsible for the security education and training program may expand or modify the coverage provided in this directive according to the agency's program and policy needs.

(b) *Elements of initial coverage.* All cleared agency personnel shall receive initial training on basic security policies, principles and practices. Such training must be provided in conjunction with the granting of a security clearance, and prior to granting access to classified information. The following areas should be considered for inclusion in initial briefings.

(1) *Roles and responsibilities.*

(A) What are the responsibilities of the senior agency official, classification management officers, the security manager and the security specialist?

(B) What are the responsibilities of agency employees who create or handle classified information?

(C) Who should be contacted in case of questions or concerns about classification matters?

(2) *Elements of classifying and declassifying information.*

(A) What is classified information and why is it important to protect it?

(B) What are the levels of classified information and the damage criteria associated with each level?

(C) What are the prescribed classification markings and why is it important to have classified information fully and properly marked?

(D) What are the general requirements for declassifying information?

(E) What are the procedures for challenging the classification status of information?

(3) *Elements of safeguarding.*

(A) What are the proper procedures for safeguarding classified information?

(B) What constitutes an unauthorized disclosure and what are the penalties associated with these disclosures?

(C) What are the general conditions and restrictions for access to classified information?

(D) What should an individual do when he or she believes safeguarding standards may have been violated?

(c) *Specialized security education and training.* Original classifiers, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information should receive more detailed training. This training should be provided before or concurrent with the date the employee assumes any of the positions listed above, but in any event no later than six months from that date. Coverage considerations should include:

(1) *Original classifiers.*

(A) What is the difference between original and derivative classification?

(B) Who can classify information originally?

(C) What are the standards that a designated classifier must meet to classify information?

(D) What is the process for determining duration of classification?

(E) What are the prohibitions and limitations on classifying information?

(F) What are the basic markings that must appear on classified information?

(G) What are the general standards and procedures for declassification?

(2) *Declassification authorities other than original classifiers.*

(A) What are the standards, methods and procedures for declassifying information under Executive Order 12958?

(B) What are the standards for creating and using agency declassification guides?

(C) What is contained in the agency's automatic declassification plan?

(D) What are the agency responsibilities for the establishment and maintenance of a declassification database?

(3) *Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information.*

(A) What are the original and derivative classification processes and the standards applicable to each?

(B) What are the proper and complete classification markings, as described in Subpart B of this directive?

(C) What are the authorities, methods and processes for downgrading and declassifying information?

(D) What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

(E) What are the requirements for creating and updating classification and declassification guides?

(F) What are the requirements for controlling access to classified information?

(G) What are procedures for investigating and reporting instances of security violations, and the penalties associated with such violations?

(H) What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

(I) What are the procedures for the secure use, accreditation and certification of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

(J) What are the requirements for oversight of the security classification program, including agency self-inspections?

(d) *Refresher security education and training.* Agencies shall provide refresher training to employees who create, process or handle classified information. Refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during agency self-inspections. When other methods are impractical, agencies may satisfy the requirement for refresher training by means of audiovisual products or written materials.

(e) *Termination briefings.* Each agency shall ensure that each employee granted access to classified information who leaves the service of the agency receives a termination briefing. Also, each agency employee whose clearance is withdrawn must receive such a briefing. At a minimum, termination briefings must impress upon each employee: (1) the continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance; and (2) the obligation to return to the appropriate agency official all classified documents and materials in the employee's possession.

(f) *Other security education and training.* Agencies are encouraged to develop additional security education and training according to program and policy needs. Such security education and training could include: (1) practices applicable to U.S. officials traveling overseas; (2) procedures for protecting classified information processed and stored in automated information systems; (3) methods for dealing with uncleared personnel who work in proximity to classified information; (4) responsibilities of personnel serving as couriers of classified information; and (5) security requirements that govern participation in international programs.

Subpart E—Declassification

§2001.50 Definitions [3.1]

(a) *Permanently valuable information.* "Permanently valuable information" or "permanent historical value" refers to information contained in: (1) records that have been accessioned into the National Archives of the United States; (2) records that have been scheduled as permanent under a records retention schedule approved by the National Archives and Records Administration (NARA); and (3) presidential historical materials,

presidential records or donated historical materials located in the National Archives of the United States, a presidential library, or any other approved repository.

(b) *File series.* A "file series" is a body of related records created or maintained by an agency, activity, office or individual. The records may be related by subject, topic, form, function, or filing scheme. An agency, activity, office, or individual may create or maintain several different file series, each serving a different function. Examples may include a subject file, alphabetical name index, chronological file, or a record set of agency publications. File series frequently correspond to items on a NARA-approved agency records schedule. Some very large series may contain several identifiable sub-series, and it may be appropriate to treat sub-series as discreet series for the purposes of the Order.

§2001.51 Automatic declassification [3.4]

(a) *General.* All departments and agencies that have original classification authority, or previously had original classification authority, and maintain records appraised as having permanent historical value that contain information classified by that agency shall comply with the automatic declassification provisions of the Order. All agencies with original classification authority shall cooperate with NARA in carrying out an automatic declassification program involving accessioned Federal records, presidential papers and records, and donated historical materials under the control of the Archivist of the United States.

(b) *Presidential records.* The Archivist of the United States shall establish procedures for the declassification of presidential or White House materials accessioned into the National Archives of the United States or maintained in the presidential libraries.

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

(d) *Unofficially transferred information.* In the case of classified information that is not officially transferred as described in paragraph (c), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, the Director of ISOO will designate an agency or agencies to act on provisions of the Order.

(e) *Processing records originated by another agency.* When an agency uncovers classified records originated by another agency that appear to meet the criteria for the application of the automatic declassification provisions of the Order, the finding agency should alert the originating agency and seek instruction regarding the handling and disposition of pertinent records.

(f) *Unscheduled records.* Classified information in records that have not been scheduled for disposal or retention by NARA is not subject to section 3.4 of the Order. Classified information in records that are scheduled as permanently valuable when that information is already more than 20 years old shall be subject to the automatic declassification provisions of section 3.4 of the Order five years from the date the records are scheduled. Classified information in records that are scheduled as permanently valuable when that information is less than 20 years old shall be subject to the automatic declassification provisions of section 3.4 of the Order when the information is 25 years old.

(g) *Foreign government information.* When foreign government information appears to be subject to automatic declassification, the declassifying agency shall determine whether: (1) the information is subject to a treaty or international agreement that would prevent its declassification at that time; or (2) another exemption under section 3.4(b) of the Order applies to the information. If no exemption appears to apply, the declassifying agency or the Department of State, as appropriate, ordinarily should consult with the foreign government prior to declassification.

(h) *Assistance to the Archivist of the United States.* Agencies shall consult with NARA before establishing automatic declassification programs. Agencies shall cooperate with NARA in developing schedules for the declassification of records in the National Archives of the United States and the presidential libraries to ensure that declassification is accomplished in a timely manner. NARA will provide information about the records proposed for automatic declassification. Agencies shall consult with NARA before reviewing records in their holdings to ensure that appropriate procedures are established for maintaining the integrity of the records and that NARA receives accurate information about agency declassification actions when records are transferred to NARA. NARA will provide guidance to the agencies about the requirements for notification of declassification actions on transferred records, box labeling, and identifying exempt information in the records.

(i) *Use of approved declassification guides.* Approved declassification guides may be used as a tool to assist in the exemption from automatic declassification of specific information as provided in section 3.4(d) of the Order. These guides must include additional pertinent detail relating to the exemptions described in section 3.4(b) of the Order, and follow the format required of declassification guides for systematic review as described in §2001.53 of this directive. In order for such guides to be used in place of the identification of specific information within individual documents, the information to be exempted must be narrowly defined, with sufficient specificity to allow the user to identify the information with precision. Exemptions for general categories of information will not be acceptable. The actual items to be exempted are specific documents. All such declassification guides used in conjunction with section 3.4(d) of the Order must be submitted to the Director of ISOO, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, for approval by the Panel.

(j) *Automatic declassification date.* No later than April 17, 2000, information over 25 years old in unreviewed permanently valuable records in non-exempt file series will be automatically declassified.

(k) *Redaction standard.* Agencies are encouraged but are not required to redact documents that contain information that is exempt from automatic declassification under section 3.4 of the Order, especially if the information that must remain classified comprises a relatively small portion of the document

§2001.52 Systematic declassification review [3.5]

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

(b) *Responsibilities.* Agencies shall establish systematic review programs for those records containing information that is exempt from automatic declassification. Agencies may also conduct systematic review of information contained in permanently valuable records that is less than 25 years old.

§2001.53 Declassification guides [3.5(b)]

(a) *Preparation of declassification guides.* Declassification guides shall be prepared to facilitate the declassification of information contained in records determined to be of permanent historical value.

(b) *General content of declassification guides.* Declassification guides shall, at a minimum:

- (1) identify the subject matter of the declassification guide;
- (2) identify the original declassification authority by name or personal identifier, and position;
- (3) provide the date of issuance or last review;
- (4) state precisely the categories or elements of information:
 - (A) to be declassified;
 - (B) to be downgraded; or
 - (C) not to be declassified.
- (5) identify any related files series that have been exempted from automatic declassification pursuant to section 3.4(c) of the Order;
- (6) to the extent a guide is used in conjunction with the automatic declassification provisions in section 3.4 of the Order, state precisely the elements of information to be exempted from declassification to include:
 - (A) the appropriate exemption category listed in section 3.4(b) of the Order, and, when citing the exemption category listed in section 3.4(b)(9) of the Order, specify the applicable statute, treaty or international agreement; and
 - (B) a date or event for declassification.

(c) *External review.* Agencies shall submit declassification guides for review to the Director of ISOO. To the extent such guides are used in conjunction with the automatic declassification provisions in section 3.4 of the Order, the Director shall submit them for approval by the Interagency Security Classification Appeals Panel.

(d) *Internal review and update.* Agency declassification guides shall be reviewed and updated as circumstances require, but at least once every five years. Each agency shall maintain a list of its declassification guides in use.

§2001.54 Mandatory review for declassification [3.6, 3.7]

(a) *U.S. originated information.*

(1) *Receipt of requests.* Each agency shall publish in the Federal Register the identity of the person(s) or office(s) to which mandatory declassification review requests should be addressed.

(2) *Processing.*

(A) *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 specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. 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 ordinarily make a final determination within 180 days from the date of receipt. 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 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.

(B) *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 refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that the custodial agency may review its records, the custodial agency shall review the requested records in accordance with declassification guides or guidelines provided by the originating agency. Upon receipt of a request from the referring agency, the originating agency shall process the request in accordance with this section. The originating agency shall communicate its declassification determination to the referring agency.

(C) *Appeals of denials of mandatory declassification review requests.* The agency appellate authority shall normally make a determination within 60 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.

(D) *Appeals to the Interagency Security Classification Appeals Panel.* In accordance with section 5.4 of the Order, the Interagency Security Classification Appeals Panel shall publish in the Federal Register no later than February 12, 1996, the rules and procedures for bringing mandatory declassification appeals before it.

(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 this section. 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. The deciding agency or the Department of State, as appropriate, should ordinarily consult with the foreign government 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 12356 shall remain in effect until revised.

(e) *Assistance to the Department of State.* 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 materials in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

(f) *Requests filed under mandatory declassification review and the Freedom of Information Act.* When a requester submits a request both under mandatory review and the Freedom of Information Act (FOIA), the agency shall require the requester to elect one process or the other. If the requester fails to elect one or the other, the request will be treated as a FOIA request unless the requested materials are subject only to mandatory review.

(g) *FOIA and Privacy Act requests.* Agency heads shall process requests for declassification that are submitted under the provisions of the FOIA, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

(h) *Redaction standard.* Agencies shall redact documents that are the subject of an access demand unless the overall meaning or informational value of the document is clearly distorted by redaction.

Subpart F—Reporting

§2001.60 Statistical reporting [5.3]

Each agency that creates or handles classified information shall report annually to the Director of ISOO statistics related to its security classification program. The Director will instruct agencies what data elements are required, and how and when they are to be reported.

§2001.61 Accounting for costs [5.6(c)(8)]

(a) Information on the costs associated with the implementation of the Order will be collected from the agencies through a reporting requirement in the Government's budget process. OMB will collect the cost estimates through OMB Circular A-11, "Preparation and Submission of Budget Estimates." OMB will provide data to ISOO on the cost estimates for classification-related activities. ISOO will include these cost estimates in its annual report to the President. The agency senior official should work closely with the agency comptroller to ensure that the best estimates are collected.

(b) The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under Executive Order 12829, will collect cost estimates for classification-related activities of contractors, licensees, certificate holders, and grantees, and report them to ISOO annually. ISOO will include these cost estimates in its annual report to the President.

§2001.62 Publication and effective date [6.2]

Part 2001 shall be published in the Federal Register. It shall become effective October 14, 1995.

Date .

ACTION

MEMORANDUM FOR ANTHONY LAKE

THROUGH: R. RAND BEERS

FROM: EDWARD J. APPEL

SUBJECT: Implementing Directive for Executive Order 12958,
"Classified National Security Information"

*JB -
see E-mails.
Will need to
be revised*

Attached at Tab I for your signature is a memorandum for OMB, attention Information Security Oversight Office (ISOO), and at Tab II a letter dated September 19, 1995 from OMB with draft guidelines implementing EO 12958.

EO 12958 directs OMB, through ISOO, to issue implementing directives binding on all agencies in four specified areas. ISOO's draft guidelines were forwarded after interagency coordination. Final interagency approval is expected to occur at a meeting of the Security Policy Forum on September 29, 1995. OMB asks for our response by October 2, 1995, so that the guidelines can be printed in the Federal Register and become effective October 14, 1995.

A review of the guidelines shows that they are complete, sufficient, clear and meet the requirements of the EO. However, in focusing on foreign government information, the draft guidelines could be misconstrued by a declassifier who might not realize the necessity to apply exemptions or consult with the foreign government involved prior to final action. As you may be aware, our Australian allies (through a meeting with Sandy Berger), British and other close allies have expressed strong concerns about both the EO and draft guidelines. It has always been a prerequisite that consultation precedes release or declassification of information from highly sensitive, classified sources, projects and exchanges with our close allies. Many bilateral and multilateral agreements apply. The Australians, through Ambassador Donald Russell and Graham Kearns, Defense Policy Counsellor, expressed a need to strengthen the guidelines in discussions with both the NSC and ISOO.

The attached letter to OMB through ISOO recommends revisions to the three references to foreign government information in the draft guidelines. Should additional changes to the current text

provide
result from the September 29 meeting, NSC will be advised and will ~~review~~ those changes ~~for~~ your concurrence, prior to implementation.

Concurrence by: Alan Kreczko William Leary

RECOMMENDATION:

That you sign the letter to OMB through ISOO at Tab I.

Attachments

Tab I Memorandum to OMB through ISOO

Tab II Incoming correspondence from OMB

MEMORANDUM FOR ALICE M. RIVLIN
DIRECTOR
OFFICE OF MANAGEMENT AND BUDGET

ATTENTION:
STEVEN GARFINKEL, DIRECTOR
INFORMATION SECURITY OVERSIGHT OFFICE

SUBJECT: Implementing Directive for
Executive Order 12958, "Classified
National Security Information"

Thank you for the opportunity to review the draft guidelines transmitted with your September 19, 1995 letter.

Review of the draft Implementing Directive for Executive Order 12958 showed it to be an excellent document. You are requested to make the following changes (set out in legislative style, showing deletions lined out and recommended language in bold):

Page 3, Section 2001.12(c):

(c) *Foreign Government Information.* When foreign government information is being considered for declassification or appears to be subject to automatic declassification, **the declassifying agency shall determine whether: (1) the information is subject to a treaty or international agreement that would prevent its declassification at that time; or (2) another exemption under section 3.4(b) of the Order applies to the information.** If no exemption appears to apply, ~~ordinarily~~ the classifying agency or the Department of State, as appropriate, ~~should~~ **shall** consult with the foreign government prior to declassification.

P. 28, Section 2001.51(g):

(g) *Foreign government information.* When foreign government information appears to be subject to automatic declassification, the declassifying agency shall determine whether: (1) the information is subject to a treaty or international agreement that would prevent its declassification at that time; or (2) another exemption under section 3.4(b) of the Order applies to the information. If no exemption appears to apply, the declassifying agency or the Department of State, as appropriate,

~~ordinarily should~~ **shall** consult with the foreign government prior to declassification.

P. 32, Section 2001.54(b):

(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 this section. 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. The deciding agency or the Department of State, as appropriate, ~~should ordinarily~~ **shall** consult with the foreign government prior to final action on the request.

The above changes are requested to improve guidelines for declassification of sensitive foreign government information, emphasizing the need for prior consultation with the foreign governments involved. Several allies have pointed out that such consultation is a prerequisite of sharing this information.

Please consult with me through my staff, if further substantive changes to the directive are considered.

Anthony Lake
Assistant to the President
for National Security Affairs



13221 Woodland Park Road
Herndon, VA 22071

November 29, 1995

Please file
White House
or NSC
Security.

Viet D. Dinh
Associate Special Counsel
United States Senate
Committee on Banking, Housing and Urban Affairs
Washington, DC 20510-6075

Dear Mr. Dinh:

Sprint hereby responds to your revised subpoena dated November 21, 1995. That subpoena requested production by November 27, 1995, of:

...all records in whatever format, that reflect or relate to any telephone call or other communication from any telephone or other communication device located at the White House between May 1 and November 30, 1993.

Pursuant to discussions with Ms. Sally Smith, Sprint's Assistant Vice President for Government Affairs, the return date for the subpoena was, by your letter of November 22, 1995, modified to November 29, 1995. In addition, your letter of November 22 indicated that Sprint's production in response to the subpoena would be deemed complete if it was limited to calls placed from the White House to telephones in the 501 area code.

Enclosed find Sprint's records in response to your subpoena of November 21, 1995, as modified by your letter dated November 22, 1995. As explained in our discussions of November 22, 1995, pursuant to a customer request in 1989, Sprint "masks" or deletes the last four digits of both the originating and terminating numbers for all traffic originating out of the White House. At your request, I have researched how this "masking" process takes place to assure that complete records do not somewhere exist within Sprint.

Specifically, the White House PBX transmits all call data (all ten digits) to Sprint's DMS250 switch. The switch retains all call data and periodically downloads all data into Sprint's Message Processing System (MPS). MPS is a mainframe computer billing system located in Dallas, Texas, that performs a series of step functions which screens the raw call data information to eventually produce a "to bill" file. On receipt of the raw call data from the switch, the MPS first creates an "all calls" file. It is at this first step that the MPS is programmed to delete the last four digits of the "calling" and "called to" numbers

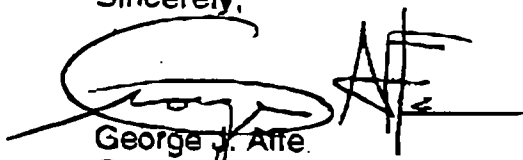
page 2

for all traffic originating from the two assigned White House exchanges. This programming is repeated in the second step of the MPS process to assure that the deletion is performed. Therefore, there is no file or system within Sprint's billing system which retains complete call detail data on the two White House exchanges.

While the complete raw call detail information is retained by the switch, it retains that complete data for only a thirty-day period. Therefore, complete call detail information for calls originating from the White House from May 1, 1993 through November 30, 1993 does not exist anywhere within Sprint.

The enclosed information, however, contains the first six digits of the "calling" and "called to" exchanges for all traffic originating in the White House from May 1 through November 30, 1993, and terminating to the 501 area code. Additionally, it should be noted that the enclosed records indicate that only one of the two exchanges (202-395) completed calls to the 501 area code during the period in question.

Sincerely,



George J. Affe
General Attorney



13221 Woodland Park Road
Herndon, VA 22071

October 2, 1995

Ms. Sheryl Hall
Title
Executive Office of The President
Office of Administration
New Executive Office Building
Washington, D.C. 20503

Dear Sheryl,

Pursuant to your request for Call Detail Records (CDR) for the month of July 1993, I have been advised by the Sprint Billing Department that these records are not available. This is due to a prior letter from the Executive Office of The President, which requested Sprint to suppress and erase the CDR.

I have requested the Sprint Contracts Department to retrieve and duplicate this letter for you. This is going to take more time because I am not sure of the date of this letter and the Contracts Department files all documents chronologically. I will call you later this week with a status.

If you have any questions, please call me at (703) 904-2303.

Sincerely,

A handwritten signature in cursive script that reads "Sheila E. Hayes".

Sheila E. Hayes
Government Account Manager

RF
KE

FEB 12 1990

The Honorable
Hector F. Irastorza, Jr.
Special Assistant to the President
and Deputy Director of the
Office of Administration
White House
Washington, DC 20500

Dear Mr. Irastorza:

Thank you for your letter of January 18, 1990, which requests my agreement to the points in Mr. Paul Bateman's letter of August 10, 1989. I believe, based on our meeting of December 21, 1989, with you and your staff, that we have reached an agreement on all points.

Listed below are the four issues and our understanding of their disposition:

1. The Executive Office of the President understands that there will be no change in the flat rate billing method presently used between the White House and the General Services Administration (GSA) for telephone service.

GSA agrees that we will bill the White House at a flat rate each fiscal year. Although the flat will not be adjusted during the fiscal year, an adjustment based on prior year usage (increase or decrease) will be made the following fiscal year.

2. The Executive Office of the President understands that no information will be collected about calls to or from the White House complex and all United States Secret Service security requirements will be met.

GSA agrees to the four specific recommendations that resulted from the meeting held on October 24, 1989, when the Secret Service Technical Security Division met with representatives of GSA and SPRINT to discuss security issues.

3. The Executive Office of the President understands that the functions, capacity, response, and reliability of their telephone service will at least equal that which they now enjoy.

- 2 -

The transition from the current FTS service to FTS2000 should remain transparent to the Federal agencies located in the White House complex. There will be no change in the service received today, only improved service under FTS2000.

4. The Executive Office of the President understands that the total cost, over time, for identical services, will be no higher than under the present system.

The cost for FTS2000 service, on a per minute basis, will be substantially below the current rate. We anticipate that the flat rate charge for fiscal year 1991 will be lower than the current FTS flat rate charge. However, if FTS2000 usage were to increase substantially during fiscal year 1991 the flat rate for fiscal year 1992 would be adjusted accordingly.

I hope GSA's position on the four points has been stated to your satisfaction. We look forward to a smooth transition to FTS2000 and your continued support in this effort. If you have any questions, please have Mr. Al Nagy contact Ms. Patricia Petroff, of my staff, on 523-4635 for assistance.

Sincerely,

SIGNED

Michael L. Corrigan

Michael L. Corrigan
Assistant Commissioner for
Telecommunications Services

cc: Official File - KBL
Reading File - KBL, KB, K

P.Petroff:dls:WH.LTR.:523-5308:2/7/90



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF ADMINISTRATION
Washington, D.C. 20503

January 18, 1990

RECEIVED
1-21-90

KB

Dear Mr. Corrigan:

Thank you for meeting with Al Nagy and David Stonehill on December 21 to discuss the FTS 2000 system. As was mentioned at that meeting, we need to present your agreement to the points in Paul Bateman's letter of August 10, 1989, to Mr. Hopf before the Executive Office of the President can sign an agreement to use the FTS 2000 system.

- "1) We understand there will be no change in the flat rate billing method presently used between the White House and GSA for telephone service.
- 2) We understand that no information will be collected about calls to or from the White House complex and all United States Secret Service security requirements will be met.
- 3) We understand that the functions, capacity, response, and reliability of our telephone service will at least equal that which we now enjoy.
- 4) We understand that the total cost, over time, for identical services, will be no higher than under the present system."

We have discussed and corresponded on these points several times since that letter, but we have no direct written assurance that they are agreed upon by the General Services Administration (GSA). A point-by-point agreement must be on record before we sign for the service. The issues of flat rate billing and security are particularly important.

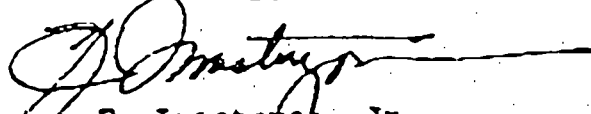
The issue of security has been further defined in our discussions. On October 24, the Secret Service Technical Security Division (TSD) met with representatives of Sprint and GSA to discuss security issues. Four specific recommendations followed from that meeting which, together, would satisfy point two in Mr. Bateman's letter. They are:

- 1) Bell Atlantic should modify the White House DMS-100 switch to send only generic ANI digits to the FTS 2000 network. This would protect the identity of the calling party. Billing would be accomplished by trunk usage metering which is compatible with the Office of Administration approach for flat rate billing.

- 2) GSA should restrict the call detailing feature within the FTS 2000 network. This eliminates the archiving of called number records from the White House extensions.
- 3) The Secret Service (TSD) should be provided access to an Administrative System for verifying service order data (quality monitoring) pertaining to the White House account.
- 4) GSA and all carriers should submit all changes in service, lines, trunks, equipment, Administrative Systems, data services and features for review and approval by the Secret Service in writing before being offered to and put into service in the White House complex.

We have discussed the FTS 2000 system for five months. I believe the issues are clear. We would like to proceed and we look forward to agreement with GSA on the four specific points in Mr. Bateman's letter.

Sincerely,



Hector F. Irastorza, Jr.
Special Assistant to the President
and Deputy Director of the
Office of Administration

Mr. Michael L. Corrigan
Deputy Commissioner for Telecommunications Services
General Services Administration
Washington, DC 20405



DEPARTMENT OF THE TREASURY
UNITED STATES SECRET SERVICE
TECHNICAL SECURITY DIVISION
WASHINGTON, DC 20223

November 16, 1989

MEMORANDUM

TO : Paul Bateman
Deputy Assistant to the President

FROM : Clint L. Howard
Special Agent in Charge
Technical Security Division

SUBJECT : FTS-2000

On October 24, 1989, SS Arnold Johnson of this division met with representatives of General Services Administration (GSA) and U.S. Sprint at the GSA Service Oversight Center (SOC). Mr. Norry Hersey of U.S. Sprint provided Mr. Joe Seanor of GSA and SS Johnson with an overview of the SOC procedures for the collection and processing of billing information of the FTS-2000 White House account. The following topics were addressed:

1. The collection of Automatic Number Identification (ANI) information about FTS calls from the White House Complex.
2. Review the SOC billing procedures and facilities to ensure that sensitive White House billing information is adequately protected.

After reviewing the FTS-2000 capabilities and facilities we recommend the following actions:

1. Bell Atlantic be instructed to modify the White House DMS-100 switch to send only generic ANI digits to the FTS-2000 network. This would protect the identity of the calling party. Billing would be accomplished by trunk usage metering which is compatible with the OA request for flat rate billing.

-2-

2. GSA be instructed to restrict the call detailing feature within the FTS-2000 network. This eliminates the archival of called number records from the White House extensions.
3. The Secret Service (TSD) be provided access to an Administrative System for verifying service order data (Quality Monitoring) pertaining to the White House account.
4. GSA and all carriers be instructed that all changes in service, lines, trunks, equipment, Administrative Systems, data services and features be reviewed and approved by the Secret Service in writing before being offered to and put into service in the White House complex.

If you have any questions please contact SS Arnie Johnson at (202) 395-6396.

Clint L. Howard
Clint L. Howard

cc: Al Nagy - OA
Joe Seanor - GSA