

PRD-29: TASK FORCE MEETING

May 13, 1993

AGENDA

- I. Welcome and introductions
- II. Overview of the task
- III. Task Force time line
- IV. Committees: Composition and taskings
- V. Committees: Process for input, analysis and reporting
- VI. Media inquiries
- VII. Congressional inquiries
- VIII. Wrap-up
- IX. Break-up into committees

LIST OF ATTACHMENTS

1. PRD 29 TASK FORCE TIME LINE
2. NAMES, ASSIGNMENTS AND COMPOSITION
OF TASK FORCE COMMITTEES
3. PROPOSALS TO BE CONSIDERED BY THE PRD 29
TASK FORCE
4. FORMAT FOR COMMITTEE INPUTS
5. PRD 29

Clinton Presidential Records Digital Records Marker

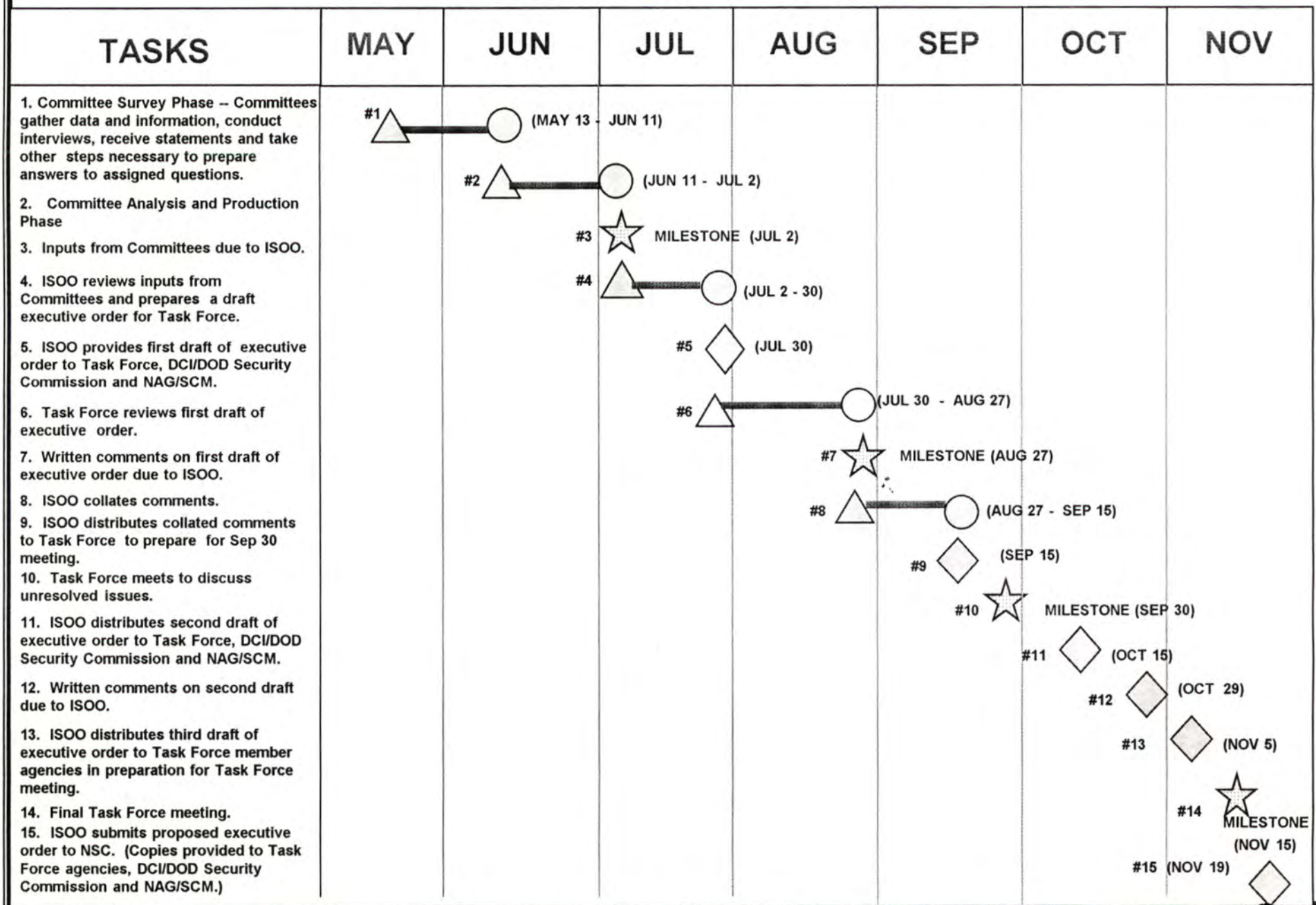
This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

1

Divider Title: _____

PRD 29 TASK FORCE TIMELINE



Clinton Presidential Records Digital Records Marker

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

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

2

Divider Title: _____

NAMES, ASSIGNMENTS AND COMPOSITION OF TASK FORCE COMMITTEES

Committee Name and Questions to be Answered	Committee Composition
Committee on Classification Standards In the post Cold War era, what types of information continue to require protection through classification in the interest of our national security? Do we need three levels of classification?	Chair: OSD Deputy Chair: Ethel R. Theis, ISOO Members: Air Force, CCISCMO, OMB
Committee on Excessive Classification What steps can be taken to avoid excessive classification?	Chair: DOE Deputy Chair: Rudy Waddy, ISOO Members: DIA, Marine Corps, Treasury
Committee on Duration of Classification What steps can be taken to declassify information as quickly as possible?	Chair: STATE Deputy Chair: Glenn Schlarman, ISOO Members: FEMA, NAVY, NRC
Committee on Declassification What steps can be taken to declassify information or otherwise dispose of the large amounts of classified information that currently exist in Government archives and other repositories?	Chair: NARA <i>mike kurtz</i> Deputy Chair: Emily R. Hickey, ISOO Members: Commerce, FBI

NAMES, ASSIGNMENTS AND COMPOSITION OF TASK FORCE COMMITTEES (cont.)

Committee Name and Questions to be Answered	Committee Composition
Committee on Oversight What steps can be taken to reduce the number of, and to provide adequate oversight and control over, special access programs? What steps can be taken to increase individual accountability for the operation of the classification system? What steps can be taken to improve oversight of the classification program generally?	Chair: DOJ Deputy Chair: Laura Kimberly, ISOO Members: DODSI, DOT
Committee on Access and Dissemination What steps can be taken to control unnecessary distribution and reproduction of classified information? What steps can be taken to enforce the "need-to-know" principle?	Chair: CIA Deputy Chair: Michael Jewell, ISOO Members: Army, OPM
Committee on Safeguards In what ways should the revised executive order on classification address information systems security? What requirements, restrictions and other safeguards should specifically be addressed in the executive order taking into account: (i) damage from unauthorized disclosures; (ii) existing or anticipated threats; and (iii) the short and long-term costs of the requirements, restrictions, or other safeguards?	Chair: NSA Deputy Chair: Philip Calabrese, ISOO Members: Coast Guard, DIS

Clinton Presidential Records Digital Records Marker

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

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

3

Divider Title: _____

**PROPOSAL TO BE CONSIDERED
BY THE
PRD 29 TASK FORCE**

COMMITTEE ON CLASSIFICATION STANDARDS

Listing the standards or "tests" for original classification at the beginning of the Order. (Section 1.1.)

Rationale: Currently, the four standards or "tests" that must be met before information may be classified in the first instance are scattered throughout E.O. 12356. Logically, these standards should be listed together to help establish the framework for original classification and, in turn the security classification system. By listing them at the beginning of the Order, improvements can be expected in avoiding unauthorized or unnecessary classification decisions; in increasing awareness about the framework of the classification system; and in enhancing classification management.

**PROPOSALS TO BE CONSIDERED
BY THE
PRD 29 TASK FORCE**

COMMITTEE ON EXCESSIVE CLASSIFICATION

1. Clarifying the circumstances under which information may be classified following an authorized disclosure. (Section 1.6.)

Rationale: The current use of the word "reclassify" suggests that such a classification action may only be authorized for information that at one time was classified and later declassified. In fact, this extraordinary action might be exercised under the proper circumstances for any information that has been previously disclosed under appropriate authority.

2. Establishing an effective mechanism for challenging improper classification. (No comparable section.)

Rationale: While E.O. 12356 encourages persons who believe information is improperly classified to bring this to the attention of responsible officials, this mechanism is not working effectively. For the most part, employees will not challenge classification decisions that they believe to be incorrect for fear of retaliation. This suggests the need for establishing an effective means for employees to challenge improper classification decisions without fear of retribution. Such a mechanism would enhance the credibility and internal agency oversight of the classification system and increase incentives for employees to challenge improper classification decisions.

3. Defining procedures to be followed in creating classified working papers. (Section 1.5.)

Rationale: Although classified working papers are commonly found throughout the executive branch, a Government-wide policy concerning how such papers should be handled and marked does not currently exist. Defining procedures for the creation and handling of working papers would strengthen controls over classified information and help prevent unnecessary classification.

**PROPOSALS TO BE CONSIDERED
BY THE
PRD 29 TASK FORCE**

COMMITTEE ON DURATION OF CLASSIFICATION

1. Rewording the requirement to seek a specific date or event for declassification. (Section 1.4.)

Rationale: Too often, original classifiers apply the "OADR" duration marking by rote. There needs to be more emphasis on the original classifier's responsibility to attempt to establish a specific date or event for declassification before resorting to an indefinite duration of classification that requires a detailed review by the originating agency.

2. Requiring a confirmation of indefinite classification before disseminating 10-year old information as a mechanism to control the use of the indefinite duration of classification. (No comparable section.)

Rationale: Only a small percentage of classified information remains "active" after ten years; further, at that time the declassification of the information or the establishment of a specific date or event is a far more likely outcome. While "OADR" avoids the problems associated with the "six year automatic declassification" (E.O. 12065) or the "General Declassification Schedule" (E.O. 11652), it contributes significantly to the build-up of a "mountain" of older classified information. Controls on the indefinite duration of classification are necessary to avoid calls for reestablishing short, arbitrary time frames for automatic declassification and to discourage the unwarranted use of the indefinite duration of classification marking.

**PROPOSALS TO BE CONSIDERED
BY THE
PRD 29 TASK FORCE

COMMITTEE ON DECLASSIFICATION**

1. Strengthening the Archivist's capacity to improve the effectiveness of the systematic review for declassification program. (Section 3.3.)

Rationale: The period since the issuance of E.O. 12356 has witnessed a dramatic downward trend in systematic review. Two factors are partially responsible for this. One is that originating agencies do not routinely provide the Archivist with current and adequate guidelines for systematic review; the other is that originating agencies seldom designate experienced personnel to assist the Archivist in the conduct of systematic review. The vitality of systematic review for declassification is heavily dependent upon a strong program at the National Archives. Timely and adequate systematic review for declassification guidelines and agency assistance are critical for strengthening the Archivist's ability to keep pace with the massive build-up of classified material.

2. Establishing mechanisms to enhance internal systematic review for declassification programs. (Section 3.3.)

Rationale: Under E.O. 12356, agencies may or may not elect to review for declassification permanently valuable records that they have originated and which remain in their custody. Because of the voluntary character of the Order, the systematic review program of many agencies has lost its momentum and, in some cases, has come to a stop. Agencies' systematic review activity remains critical to the program's success. To reverse the decline, the need exists for a mechanism that requires agencies to conduct active systematic review of permanently valuable records that have not been accessioned into the National Archives.

COMMITTEE ON DECLASSIFICATION (CONT'D)

3. Requiring the automatic downgrading of Top Secret information accessioned into the National Archives when it becomes 30 years old and the automatic declassification of accessioned classified information when it becomes 50 years old, except as specifically exempted by the agency head. (Section 3.3.)

Rationale: Downgrading and or declassifying accessioned records as they become 30 and 50 years old would relieve significant costs and administrative burdens shouldered by the National Archives. Additionally, these actions would help to dispel the public's perception that the Government keeps information classified too long.

4. Requiring the originating agency to notify the National Archives of determinations made in processing mandatory declassification review requests or appeals for accessioned classified records. (Section 3.4.)

Rationale: Notification would allow the National Archives to manage its classified holdings better by ensuring that any information that has been declassified and released through the mandatory review process would be available to future requesters. This requirement would also enhance the credibility of the classification system in the eyes of the public.

**PROPOSALS TO BE CONSIDERED
BY THE
PRD 29 TASK FORCE**

COMMITTEE ON OVERSIGHT

1. Providing for enhanced external oversight of agencies' special access programs. (Section 4.2.)

Rationale: The ability of the Director of ISOO to implement this provision has been significantly impaired by the non-delegable requirement. Demands on the Director's time, together with the large number of special access programs, make one person monitorship an impossibility. The delegation of this authority to the ISOO analysts would include meeting any special agency clearance requirements.

2. Revitalizing the need-to-know principle by providing effective internal oversight over special access programs. (Section 4.2.)

Rationale: Due to several factors, including a perceived lack of adherence to the "need-to-know" principle, special access programs have proliferated, sometimes without guarantees of internal oversight. There needs to be a requirement that agency heads ensure effective internal oversight of such programs including biennial confirmation of their continued need.

3. Requiring annual formal reviews of each special access program to ensure compliance with the Order and its Directives and requiring documentation be maintained of each program's creation and continued need. (No comparable section.)

Rationale: Due to the reality and perception of the lack of adherence to the "need-to-know" principle, special access programs have proliferated without guarantees of commensurate internal oversight. Annual internal oversight and periodic confirmation of each program's continued need would: (i) help to eliminate unnecessary special access programs; (ii) improve management and oversight of special access programs; (iii) monitor their creation and continuation, and (iv) create greater observance of the "need-to-know" principle.

COMMITTEE ON OVERSIGHT (CONT'D)

4. Increasing the accountability of personnel significantly involved in managing classified information by identifying the management of classified information as a critical element in their performance plans. (Section 5.3.)

Rationale: Currently, most personnel that are active in information security areas are not held accountable for their responsibility to manage classified information. Much of the ineffectiveness of the current classification system can be attributed to agency personnel and senior management who are not fulfilling their responsibilities in these areas. We can increase the accountability of personnel by improving the quality of the training they receive and by appraising adherence to policies and procedures in performance contracts.

**PROPOSALS TO BE CONSIDERED
BY THE
PRD 29 TASK FORCE**

COMMITTEE ON ACCESS AND DISSEMINATION

1. Incorporating the signing of the Standard Form 312 or an approved alternative nondisclosure agreement as a condition of access. (Section 4.1.)

Rationale: Such a provision would implement the requirement established in President Reagan's National Security Decision Directive 84 that states: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access."

2. Strengthening Government control over classified information by emphasizing that classified information is not personal property. (Section 4.1.)

Rationale: Special problems arise when employees treat classified information as personal property. As a result, some employees have removed classified information from official premises without proper authority. The Order must state explicitly and unambiguously that classified information must remain under the control of the Government, thus emphasizing that private individuals cannot govern access to classified information.

3. Requiring that the record or file copy of an electronically transmitted classified message contain a properly completed "Classified by" line. (Section 1.5.)

Rationale: Requiring the "Classified by" line for all types of classified documents, no matter what medium is used to hold the information, would facilitate the speedy identification of the authority or source of classification.

COMMITTEE ON ACCESS AND DISSEMINATION (CONT'D)

4. Strengthening control over classified information by encouraging agencies to place additional restrictions upon the reproduction of Secret and Confidential information. (Section 4.1.)

Rationale: Too much classified information is reproduced without control. ISOO Directive No. 1 restricts the reproduction of **Top Secret** material but requires no controls on the reproduction of other classified material unless the originator specifically requires it. Encouraging restrictions upon the reproduction of **Secret** and **Confidential** would reduce: (i) the proliferation of classified material, (ii) the likelihood of unauthorized disclosures, and (iii) the costs associated with the reproduction of classified information. It would also increase accountability for classified information.

5. Revitalizing the need-to-know principle by requiring controls over the distribution of classified information distributed on an automatic or recurring basis. (No comparable section.)

Rationale: Widespread distribution of classified information on an automatic or recurring basis without verifying the "need-to-know" is prevalent throughout the executive branch. Establishing controls over the automatic distribution of classified information would help to save costs in reproduction and distribution and reduce the number of unauthorized disclosures.

6. Listing requirements to be met by historical researchers and former Presidential appointees in order to gain access to classified information. (Section 4.3.)

Rationale: E.O. 12356 and its implementing directives are not specific concerning the requirements for access to classified information by historical researchers and former Presidential appointees. Specifying these requirements would fill an existing gap.

**PROPOSAL TO BE CONSIDERED
BY THE
PRD 29 TASK FORCE**

COMMITTEE ON SAFEGUARDS

Strengthening requirements for the protection of classified information in automated information systems. (Section 4.1.)

Rationale: The Computer Security Act and several executive branch directives address the requirement to protect electronically stored and transmitted data. The Order must be revised to conform with these authorities.

**PROPOSAL TO BE CONSIDERED
BY ALL COMMITTEES OF THE
PRD 29 TASK FORCE**

Defining new terms and providing precise definitions for terms that currently appear in E.O. 12356 or its implementing directives but which have not been clearly defined. (Section 6.1.)

Rationale: Precise definitions for terms that are integral elements of the classification system are needed. A general understanding exists, for example, about the meaning of terms such as "security violation" and "security infraction," but neither the Order nor the ISOO Directive provide clear definitions for these and other terms. Likewise, the need exists for providing clear definitions when new terms are introduced.

Clinton Presidential Records Digital Records Marker

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

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

4

Divider Title: _____

COMMITTEE INPUT FORMAT

COMMITTEE: *State name of Committee providing input.*

QUESTION TO BE ANSWERED: *State the question.*

RECOMMENDED LANGUAGE: *Proposed language to the Executive Order, both clean copy and legislative style format.*

RATIONALE: *Provide advantages and disadvantages to recommended language.*

Clinton Presidential Records Digital Records Marker

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

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

5

Divider Title: _____

April 26, 1993

PRESIDENTIAL REVIEW DIRECTIVE

SUBJECT: National Security Information

BACKGROUND

With the end of the Cold War, we should re-evaluate our security classification and safeguarding systems, as articulated in E.O. 12356, to ensure that they are in line with the reality of the current, rather than the past, threat potential.

OBJECTIVE

The objective of this tasking is to review E.O. 12356 and other directives relating to protection of national security information with a view toward drafting a new executive order that reflects the need to classify and safeguard national security information in the post Cold War period.

QUESTIONS

The following sets forth the questions that should be addressed during this review. The resulting answers should serve as the basis for the drafting of the new proposed executive order which will be submitted upon completion of the review.

- In the post Cold War era, what types of information continue to require protection through classification in the interest of our national security?
- What steps can be taken to avoid excessive classification?
- What steps can be taken to declassify information as quickly as possible?
- What steps can be taken to declassify or otherwise dispose of the large amounts of classified information that currently exist in Government archives and other repositories?
- What steps can be taken to reduce the number of, and to provide adequate oversight and control over, special access programs?
- What steps can be taken to control unnecessary distribution and reproduction of classified information?

- What steps can be taken to enforce the "need-to-know" principle?
- What steps can be taken to increase individual accountability for the operation of the classification system?

IMPLEMENTATION

This review should be conducted under the chairmanship of the Director of the Information Security Oversight Office (ISOO) in coordination with the National Advisory Group for Security Countermeasures. Representatives of the agencies which comprise the NAG/SCM shall be included in the task force. It is further directed that this review be coordinated with the joint DCI-Secretary of Defense Security Commission.

The Chairman of the task force shall report to me through the NSC staff, Office of Intelligence Programs. The review should be completed no later than November 30, 1993, at which time a draft executive order superseding E.O. 12356 should be submitted for formal coordination.

THE WHITE HOUSE
WASHINGTON

April 26, 1993

PRESIDENTIAL REVIEW DIRECTIVE/NSC-29

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF ENERGY
THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF CENTRAL INTELLIGENCE
THE ADMINISTRATOR OF GENERAL SERVICES
THE DIRECTOR, OFFICE OF PERSONNEL MANAGEMENT
THE DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE

SUBJECT: National Security Information

BACKGROUND

With the end of the Cold War, we should re-evaluate our security classification and safeguarding systems, as articulated in E.O. 12356, to ensure that they are in line with the reality of the current, rather than the past, threat potential.

OBJECTIVE

The objective of this tasking is to review E.O. 12356 and other directives relating to protection of national security information with a view toward drafting a new executive order that reflects the need to classify and safeguard national security information in the post Cold War period.

QUESTIONS

The following sets forth the questions that should be addressed during this review. The resulting answers should serve as the basis for the drafting of the new proposed executive order which will be submitted upon completion of the review.

-- In the post Cold War era, what types of information continue to require protection through classification in the interest of our national security?

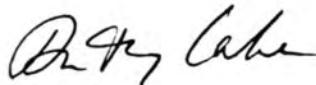
-- What steps can be taken to avoid excessive classification?

- What steps can be taken to declassify information as quickly as possible?
- What steps can be taken to declassify or otherwise dispose of the large amounts of classified information that currently exist in Government archives and other repositories?
- What steps can be taken to reduce the number of, and to provide adequate oversight and control over, special access programs?
- What steps can be taken to control unnecessary distribution and reproduction of classified information?
- What steps can be taken to enforce the "need-to-know" principle?
- What steps can be taken to increase individual accountability for the operation of the classification system?

IMPLEMENTATION

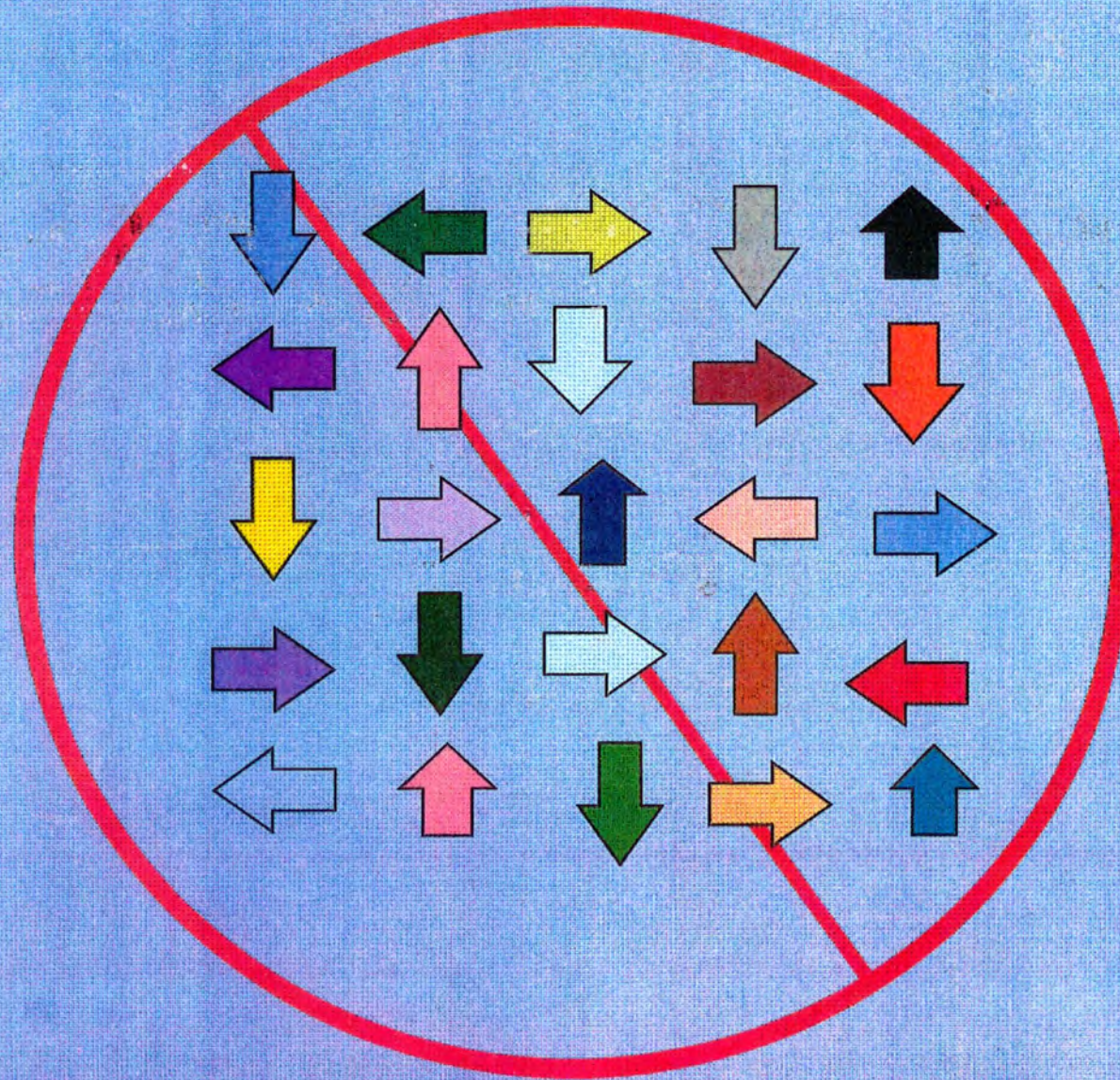
This review should be conducted under the chairmanship of the Director of the Information Security Oversight Office (ISOO) in coordination with the National Advisory Group for Security Countermeasures. Representatives of the agencies which comprise the NAG/SCM shall be included in the task force. It is further directed that this review be coordinated with the joint DCI-Secretary of Defense Security Commission.

The Chairman of the task force shall report to me through the NSC staff, Office of Intelligence Programs. The review should be completed no later than November 30, 1993, at which time a draft executive order superseding E.O. 12356 should be submitted for formal coordination.



Anthony Lake
Assistant to the President for
National Security Affairs

TWENTY FIVE ARROWS GOING IN DIFFERENT DIRECTIONS





THE VICE PRESIDENT
WASHINGTON

May 7, 1993

Richard M. Schmidt, Jr., Esq.
Allan R. Adler, Esq.
Cohn & Marks
1333 New Hampshire Avenue NW, Suite 600
Washington, D.C. 20036

Dear Messrs. Schmidt & Adler:

Thank you for sending me a copy of your proposal concerning the creation of a more informed and participatory democracy. I appreciate being informed in this way.

I am impressed with this detailed and very professional presentation. The information you provided certainly appears to contain ideas that merit careful attention. I will retain this material for future consideration as the President and I work on related policies and programs.

Once again, thank you for keeping me informed of your efforts and for bringing this proposal to my attention.

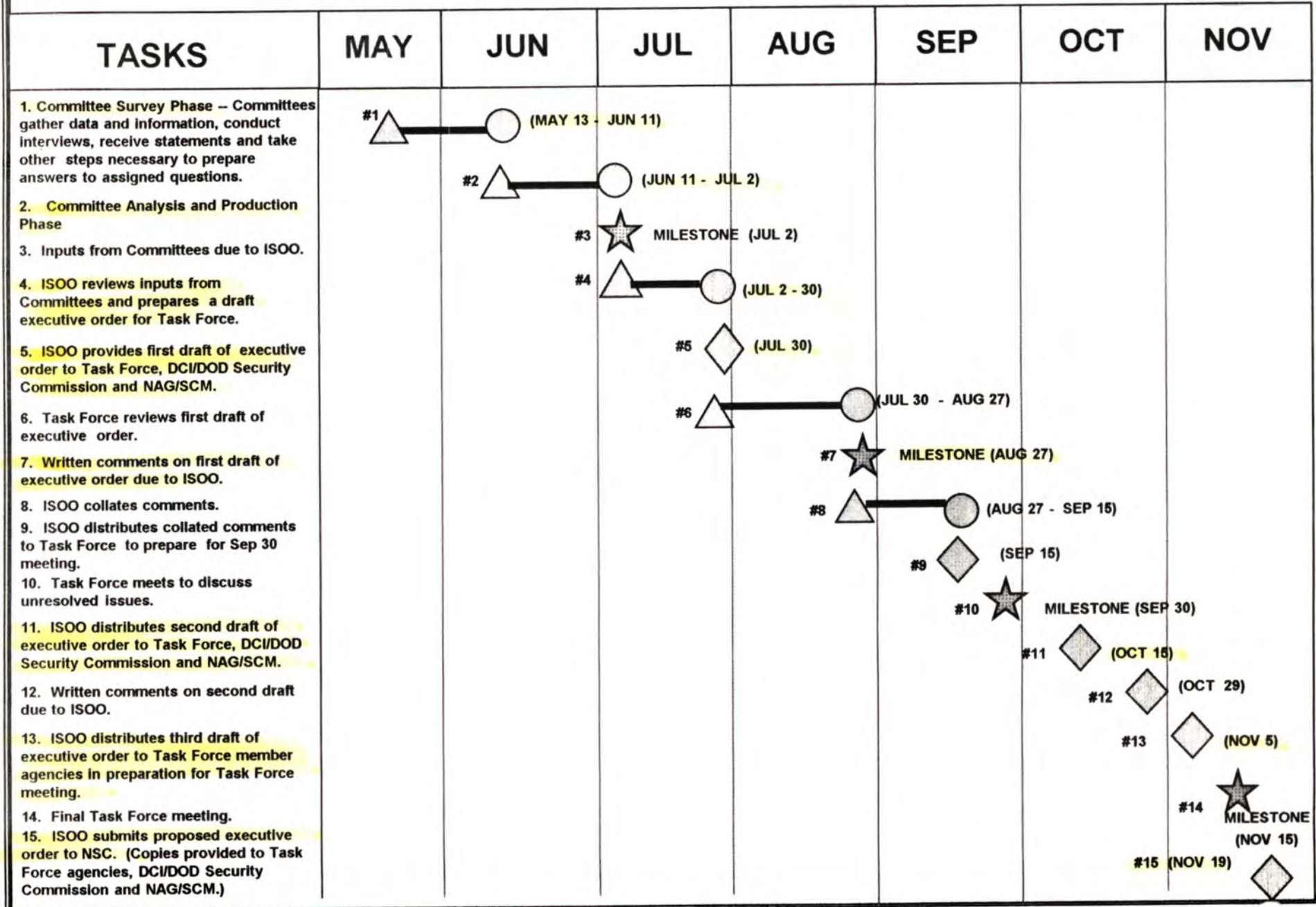
Sincerely,


Al Gore

Smith Commission [
George Tenet [
* T
Public consultation
* fully consultative
* security review organization
* contact
* charter
*

Jeff Smith
315(a)
* equality fairness
doctrine
improved

PRD 29 TASK FORCE TIMELINE



April 26, 1993

PRESIDENTIAL REVIEW DIRECTIVE

SUBJECT: National Security Information

BACKGROUND

With the end of the Cold War, we should re-evaluate our security classification and safeguarding systems, as articulated in E.O. 12356, to ensure that they are in line with the reality of the current, rather than the past, threat potential.

OBJECTIVE

The objective of this tasking is to review E.O. 12356 and other directives relating to protection of national security information with a view toward drafting a new executive order that reflects the need to classify and safeguard national security information in the post Cold War period.

QUESTIONS

The following sets forth the questions that should be addressed during this review. The resulting answers should serve as the basis for the drafting of the new proposed executive order which will be submitted upon completion of the review.

- In the post Cold War era, what types of information continue to require protection through classification in the interest of our national security?
- What steps can be taken to avoid excessive classification?
- What steps can be taken to declassify information as quickly as possible?
- What steps can be taken to declassify or otherwise dispose of the large amounts of classified information that currently exist in Government archives and other repositories?
- What steps can be taken to reduce the number of, and to provide adequate oversight and control over, special access programs?
- What steps can be taken to control unnecessary distribution and reproduction of classified information?

- What steps can be taken to enforce the "need-to-know" principle?
- What steps can be taken to increase individual accountability for the operation of the classification system?

IMPLEMENTATION

This review should be conducted under the chairmanship of the Director of the Information Security Oversight Office (ISOO) in coordination with the National Advisory Group for Security Countermeasures. Representatives of the agencies which comprise the NAG/SCM shall be included in the task force. It is further directed that this review be coordinated with the joint DCI-Secretary of Defense Security Commission.

The Chairman of the task force shall report to me through the NSC staff, Office of Intelligence Programs. The review should be completed no later than November 30, 1993, at which time a draft executive order superseding E.O. 12356 should be submitted for formal coordination.

CLASSIFICATION SYSTEM REFORM UPDATE
AND REQUEST FOR SIGNATURES ON LETTER TO PRESIDENT CLINTON

The review process initiated by President Clinton's recent Presidential Review Directive, which establishes an interagency task force to propose changes to the security information classification system, is now underway.

A working group of public interest organizations and interested individuals has been engaged for some time in compiling recommendations for changes to the government policies and procedures that have contributed to the trend towards overclassification and excessive government secrecy. The working group has drafted a formal letter to the President congratulating him for initiating this review. However, the letter also expresses concerns about the lack of a mandate for the review group to approach the problem in a way that will reverse the excessive secrecy of the past and instead ensure the greatest degree possible of public access to government information. The letter further raises grave concerns that the process as currently configured does not incorporate public input on an ongoing basis.

A copy of the letter to the President follows this memo. We urge every organization interested in the review process established by the President's directive to add its name to the letter, which we would like to send to the White House by the end of this week. Because the interagency review process is moving very quickly, we believe it is important to send the letter as soon as possible if our views are to have any impact.

If you wish to add your organization's name to the letter, please contact one of the persons listed below by Thursday noon, June 3. Please also call if you have any other questions about the review group or are interested in information about speaking at the public hearings scheduled by the interagency committees on June 9 and 10.

Contact people:

Sheryl L. Walter,
General Counsel
National Security Archive
1755 Massachusetts Ave. NW
Washington, D.C. 20036
Phone: (202) 797-0882
Fax: (202) 387-6315

Kate Martin, Director
ACLU
Center for Nat'l Security Studies
122 Maryland Ave., NE
Washington, D.C. 20002
Phone: (202) 675-2327
Fax: (202) 546-1440

May 25, 1993

June —, 1993

President Bill Clinton
The White House
Washington, D.C. 20500

Dear Mr. President:

We are a broad coalition of scholars, historians, journalists, environmentalists, and civil liberties groups who work to preserve the public's right to know and have long sought fundamental reform of the government's classification system to ensure that right. We applaud your initiation of the long-overdue and much needed review of government secrecy policy through issuance of your April 26 Presidential Review Directive on National Security Information. The Directive is an essential step towards major reform of the national security secrecy system in light of the end of the Cold War.

At the same time, we are concerned that the Directive omits mention of the core premise that must guide any review process that will effect real change: the principle that, because a vital democracy requires an informed electorate, the classification system must be designed to further the public's right to know to the greatest extent possible. In James Madison's words: "A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy or perhaps both." We urge you to direct the task force to adopt Madison's wisdom as its guiding principle. While we recognize that national security interests require that some government information be kept secret, the task force should be directed to ensure that the greatest amount of information be disclosed at the earliest possible time. This approach will help restore constitutional principles that were seriously eroded in the past in the name of fighting the Cold War.

Further, we are greatly concerned about the procedures established to perform this review. We are dismayed that there are insufficient provisions for substantive public comment and review on an ongoing basis throughout the review process. We are also skeptical that the task force as presently constituted will perform a critical appraisal of the present system and come up with innovative solutions to these very serious problems. Of particular concern to us is that the review process is not staffed by new appointees with fresh perspectives, but rather directed by those who have implemented and supported the present secrecy system for the last 12 years. We are especially worried that the Information Security Oversight Office will simply recycle with cosmetic changes the draft executive order it had prepared for the Bush Administration. We urge the creation of a formal process for ongoing public comment and review and active involvement by senior agency officials throughout the process.

Thank you for considering our views. We would be happy to meet with your staff members working on this at their earliest convenience.

American Civil Liberties Union

National Security Archive

[additional signators]

#

INFORMATION SECURITY OVERSIGHT OFFICE

Hearing: Changes to the Security Classification System

Take notice that on June 9 and 10, 1993, an interagency Task Force chaired by the Information Security Oversight Office (ISOO) will convene to hear oral presentations by interested parties on proposals to change the system under which information is classified, safeguarded, and declassified in the interest of national security. That system is currently embodied in Executive Order 12356, entitled "National Security Information," 47 FR 27836, April 6, 1982.

Background

By Presidential Review Directive, an interagency Task Force chaired by ISOO is responsible for drafting and proposing to the National Security Council no later than November 30, 1993, a security classification system to replace E.O. 12356. The Task Force has been divided into seven Committees to gather input, consider proposals, and recommend changes to be incorporated into the draft order. These Committees are as follows:

Committee on Classification Standards: This Committee is responsible for responding to the following questions: In the post Cold War era, what types of information continue to require protection through classification in the interest of our national security? Do we need three levels of classification?

Committee on Excessive Classification: This Committee is responsible for responding to the following question: What steps can be taken to avoid excessive classification?

Committee on Duration of Classification: This Committee is responsible for responding to the following question: What steps can be taken to declassify information as quickly as possible?

Committee on Declassification: This Committee is responsible for responding to the following question: What steps

can be taken to declassify or otherwise dispose of the large amounts of classified information that currently exist in Government archives or other repositories?

Committee on Access and Dissemination: This Committee is responsible for responding to the following questions: What steps can be taken to control unnecessary distribution and reproduction of classified information? What steps can be taken to enforce the "need-to-know" principle?

Committee on Oversight: This Committee is responsible for responding to the following questions: What steps can be taken to reduce the number of, and to provide adequate oversight and control over, special access programs? What steps can be taken to increase individual accountability for the operation of the classification system? What steps can be taken to improve oversight of the classification program generally?

Committee on Safeguards: This Committee is responsible for responding to the following questions: In what way should the executive order address information systems security? What requirements, restrictions, and other safeguards should be specifically addressed in the executive order taking into account (i) damage from unauthorized disclosures; (ii) existing or anticipated threats; and (iii) the short- and long-term costs of the requirements, restrictions, or other safeguards?

Purpose

To help assure that all organizations and individuals that have an interest in the security classification system have an opportunity to present their views and proposals, the Task Force Committees will convene to receive oral presentations, statements and testimony.

Location

The Great Hall, First Floor, Department of Justice Headquarters Building, Constitution Avenue, between 9th and 10th Streets, Northwest,

Washington, DC. Please enter at middle entrance on Constitution Avenue.

Times

June 9, 1993:

Committee on Classification Standards: 9-10:30 a.m.

Committee on Excessive Classification: 10:30 a.m.-noon.

Committee on Oversight: 1:30-3 p.m.

Committee on Safeguards: 3-4:30 p.m.

June 10, 1993:

Committee on Duration of Classification: 9-10:30 a.m.

Committee on Declassification: 10:30-noon.

Committee on Access and Dissemination: 1:30-3 p.m.

Times are subject to change depending on expressed interest. Parties with appointments will be notified of any changes as soon as possible.

Appointments

Oral presentations will be scheduled by appointment. To reserve an appointment time, please contact June Brown or Dorothy Cephas of ISOO, at (202) 634-6150. Presenters are requested to keep their prepared statements as concise as possible, and to provide specific written proposals for changes to particular provisions of E.O. 12356. The presentations will be open to the public.

Written Proposals

The Task Force will accept and consider written proposals for changes to E.O. 12356. Written proposals should be submitted as early as possible for adequate dissemination and consideration, but no later than July 14, 1993. Please address such proposals to the Information Security Oversight Office, 750 17th Street, NW., suite 530, Washington, DC 20006, Attention: PRD Task Force.

Steven Garfinkel,

Director, Information Security Oversight Office.

[FR Doc. 93-11942 Filed 5-19-93; 8:45 am]

BILLING CODE 6820-AF-M

INFORMATION SECURITY OVERSIGHT OFFICE

Hearing: Changes to the Security Classification System

Take notice that on June 9 and 10, 1993, an interagency Task Force chaired by the Information Security Oversight Office (ISOO) will convene to hear oral presentations by interested parties on proposals to change the system under which information is classified, safeguarded, and declassified in the interest of national security. That system is currently embodied in Executive Order 12356, entitled "National Security Information," 47 FR 27836, April 6, 1982.

Background

By Presidential Review Directive, an interagency Task Force chaired by ISOO is responsible for drafting and proposing to the National Security Council no later than November 30, 1993, a security classification system to replace E.O. 12356. The Task Force has been divided into seven Committees to gather input, consider proposals, and recommend changes to be incorporated into the draft order. These Committees are as follows:

Committee on Classification Standards: This Committee is responsible for responding to the following questions: In the post Cold War era, what types of information continue to require protection through classification in the interest of our national security? Do we need three levels of classification?

Committee on Excessive Classification: This Committee is responsible for responding to the following question: What steps can be taken to avoid excessive classification?

Committee on Duration of Classification: This Committee is responsible for responding to the following question: What steps can be taken to declassify information as quickly as possible?

Committee on Declassification: This Committee is responsible for responding to the following question: What steps

can be taken to declassify or otherwise dispose of the large amounts of classified information that currently exist in Government archives or other repositories?

Committee on Access and Dissemination: This Committee is responsible for responding to the following questions: What steps can be taken to control unnecessary distribution and reproduction of classified information? What steps can be taken to enforce the "need-to-know" principle?

Committee on Oversight: This Committee is responsible for responding to the following questions: What steps can be taken to reduce the number of, and to provide adequate oversight and control over, special access programs? What steps can be taken to increase individual accountability for the operation of the classification system? What steps can be taken to improve oversight of the classification program generally?

Committee on Safeguards: This Committee is responsible for responding to the following questions: In what way should the executive order address information systems security? What requirements, restrictions, and other safeguards should be specifically addressed in the executive order taking into account (i) damage from unauthorized disclosures; (ii) existing or anticipated threats; and (iii) the short- and long-term costs of the requirements, restrictions, or other safeguards?

Purpose

To help assure that all organizations and individuals that have an interest in the security classification system have an opportunity to present their views and proposals, the Task Force Committees will convene to receive oral presentations, statements and testimony.

Location

The Great Hall, First Floor, Department of Justice Headquarters Building, Constitution Avenue, between 9th and 10th Streets, Northwest,

Washington, DC. Please enter at middle entrance on Constitution Avenue.

Times

June 9, 1993:

Committee on Classification Standards: 9-10:30 a.m.

Committee on Excessive Classification: 10:30 a.m.-noon.

Committee on Oversight: 1:30-3 p.m.

Committee on Safeguards: 3-4:30 p.m.

June 10, 1993:

Committee on Duration of Classification: 9-10:30 a.m.

Committee on Declassification: 10:30-noon.

Committee on Access and Dissemination: 1:30-3 p.m.

Times are subject to change depending on expressed interest. Parties with appointments will be notified of any changes as soon as possible.

Appointments

Oral presentations will be scheduled by appointment. To reserve an appointment time, please contact June Brown or Dorothy Cephas of ISOO, at (202) 634-6150. Presenters are requested to keep their prepared statements as concise as possible, and to provide specific written proposals for changes to particular provisions of E.O. 12356. The presentations will be open to the public.

Written Proposals

The Task Force will accept and consider written proposals for changes to E.O. 12356. Written proposals should be submitted as early as possible for adequate dissemination and consideration, but no later than July 14, 1993. Please address such proposals to the Information Security Oversight Office, 750 17th Street, NW., suite 530, Washington, DC 20006, Attention: PRD Task Force.

Steven Garfinkel,

Director, Information Security Oversight Office.

[FR Doc. 93-11942 Filed 5-19-93; 8:45 am]

BILLING CODE 6820-AF-M

103d CONGRESS
1st Session

S. 311

IN THE SENATE OF THE UNITED STATES

Mr. Bumpers introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To amend Section 2511 of Title 18, United States Code, to make lawful the interception of an oral, wire, or electronic communication that is made with the consent of all parties to the communication.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE

This Act may be cited as "The Telephone Privacy Act of 1993".

SECTION 2. CONSENT TO INTERCEPTION OF AN ORAL,
WIRE OR ELECTRONIC COMMUNICATION

Subsection 2(d) of Sec. 2511 of Title 18 United States Code is amended to read as follows:

"2(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where

(i) all parties to the communication have given prior consent to such interception, unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States; or

ii) such person is an employer, or the officer or agent of an employer, engaged in lawful electronic monitoring of its employees' communications made in the course of the employees' duties.

Federal Register

Thursday
May 20, 1993

Part III

Information Security Oversight Office

Hearing; Changes to the Security
Classification System; Notice

INFORMATION SECURITY OVERSIGHT OFFICE

Hearing: Changes to the Security Classification System

Take notice that on June 9 and 10, 1993, an interagency Task Force chaired by the Information Security Oversight Office (ISOO) will convene to hear oral presentations by interested parties on proposals to change the system under which information is classified, safeguarded, and declassified in the interest of national security. That system is currently embodied in Executive Order 12356, entitled "National Security Information," 47 FR 27836, April 6, 1982.

Background

By Presidential Review Directive, an interagency Task Force chaired by ISOO is responsible for drafting and proposing to the National Security Council no later than November 30, 1993, a security classification system to replace E.O. 12356. The Task Force has been divided into seven Committees to gather input, consider proposals, and recommend changes to be incorporated into the draft order. These Committees are as follows:

Committee on Classification Standards: This Committee is responsible for responding to the following questions: In the post Cold War era, what types of information continue to require protection through classification in the interest of our national security? Do we need three levels of classification?

Committee on Excessive Classification: This Committee is responsible for responding to the following question: What steps can be taken to avoid excessive classification?

Committee on Duration of Classification: This Committee is responsible for responding to the following question: What steps can be taken to declassify information as quickly as possible?

Committee on Declassification: This Committee is responsible for responding to the following question: What steps

can be taken to declassify or otherwise dispose of the large amounts of classified information that currently exist in Government archives or other repositories?

Committee on Access and Dissemination: This Committee is responsible for responding to the following questions: What steps can be taken to control unnecessary distribution and reproduction of classified information? What steps can be taken to enforce the "need-to-know" principle?

Committee on Oversight: This Committee is responsible for responding to the following questions: What steps can be taken to reduce the number of, and to provide adequate oversight and control over, special access programs? What steps can be taken to increase individual accountability for the operation of the classification system? What steps can be taken to improve oversight of the classification program generally?

Committee on Safeguards: This Committee is responsible for responding to the following questions: In what way should the executive order address information systems security? What requirements, restrictions, and other safeguards should be specifically addressed in the executive order taking into account (i) damage from unauthorized disclosures; (ii) existing or anticipated threats; and (iii) the short- and long-term costs of the requirements, restrictions, or other safeguards?

Purpose

To help assure that all organizations and individuals that have an interest in the security classification system have an opportunity to present their views and proposals, the Task Force Committees will convene to receive oral presentations, statements and testimony.

Location

The Great Hall, First Floor, Department of Justice Headquarters Building, Constitution Avenue, between 9th and 10th Streets, Northwest,

Washington, DC. Please enter at middle entrance on Constitution Avenue.

Times

June 9, 1993:

Committee on Classification Standards: 9-10:30 a.m.

Committee on Excessive Classification: 10:30 a.m.-noon.

Committee on Oversight: 1:30-3 p.m.

Committee on Safeguards: 3-4:30 p.m.

June 10, 1993:

Committee on Duration of Classification: 9-10:30 a.m.

Committee on Declassification: 10:30-noon.

Committee on Access and Dissemination: 1:30-3 p.m.

Times are subject to change depending on expressed interest. Parties with appointments will be notified of any changes as soon as possible.

Appointments

Oral presentations will be scheduled by appointment. To reserve an appointment time, please contact June Brown or Dorothy Cephas of ISOO, at (202) 634-6150. Presenters are requested to keep their prepared statements as concise as possible, and to provide specific written proposals for changes to particular provisions of E.O. 12356. The presentations will be open to the public.

Written Proposals

The Task Force will accept and consider written proposals for changes to E.O. 12356. Written proposals should be submitted as early as possible for adequate dissemination and consideration, but no later than July 14, 1993. Please address such proposals to the Information Security Oversight Office, 750 17th Street, NW., suite 530, Washington, DC 20006, Attention: PRD Task Force.

Steven Garfinkel,

Director, Information Security Oversight Office.

[FR Doc. 93-11942 Filed 5-19-93; 8:45 am]

BILLING CODE 4820-AF-W

COUNCIL OF THE DISTRICT OF COLUMBIA

1350 Pennsylvania Avenue, N.W.

Washington, D.C. 20004

Memorandum

To: Members of the Council
From: Phyllis Jones, Secretary to the Council *H*
Date: March 12, 1993
Subject: Referral of Proposed Legislation

Notice is given that the attached proposed legislation has been introduced in the Office of the Secretary on March 11, 1993. Copies are available in Room 28, Legislative Services Division.

TITLE: Protection of Private Communications Amendment Act
of 1993, Bill 10-180

INTRODUCED BY: Chairman Wilson

The Chairman is referring this proposed legislation to the Committee on the Judiciary.

cc: General Counsel
Legislative Services Division

'93 MAR 11 P5:30


Chairman John A. Wilson

02

03

A BILL

04

05

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

06

07

Chairman John A. Wilson introduced the following bill, which was referred
to the Committee on _____.

08

09

To amend Title 23 of the District of Columbia Code to eliminate the 1-party
consent exception to the prohibition on eavesdropping in a non-law
enforcement case, and to allow a civil action against a person who
eavesdrops illegally.

10

11

12

13

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA,
That this act may be cited as the "Protection of Private Communications
Amendment Act of 1993".

14

15

16

Sec. 2. Title 23 of the District of Columbia Code is amended as
follows:

17

18

(a) Section 23-542(b)(3) is amended by striking the phrase "such
person is a party to the communication, or where one of the parties to
the communication has given prior consent to such interception" and

19

20

21

inserting the phrase "each party to the communication has given prior
consent to such interception;" in its place.

(b) Section 23-554(a) is amended to read as follows:

"(a) Any person whose wire, oral, or electronic communication is
intercepted, disclosed, or used in violation of this subchapter shall:

"(1) Have a civil cause of action against any person who
intercepts, discloses, or uses, or procures any other person to intercept,
disclose, or use, such communications in violation of this subchapter; and

"(2) Be entitled to recover from any such person:

"(A) Actual damages;

"(B) Punitive damages; and

"(C) Reasonable attorney's fees and other litigation costs
reasonably incurred."

Sec. 3. This act shall take effect after a 60-day period of
Congressional review following approval by the Mayor (or in the event of
veto by the Mayor, action by the Council of the District of Columbia to
override the veto) as provided in section 602(c)(2) of the District of
Columbia Self-Government and Governmental Reorganization Act, approved
December 24, 1973 (87 Stat. 813; D.C. Code § 1-233(c)(2)), and
publication in either the District of Columbia Register, the District of
Columbia Statutes-at-Large, or the District of Columbia Municipal
Regulations.

Judge of United States District Court authorized to issue wiretap orders. — Section 23-547, read together with paragraph (7) of this section, explicitly authorizes the issuance of wiretap orders by "a judge of the United States District Court for the District of Columbia." *United States v. Johnson*, 696 F.2d 115 (D.C. Cir. 1982).

Pen registers not within scope of wiretapping law. — Pen registers, which record outgoing numbers called on a particular telephone line, are not prohibited or regulated by the wiretap provisions of the District of Columbia Code. *Davis v. United States*, App. D.C., 390 A.2d 976 (1978).

§ 23-542. Interception, disclosure, and use of wire or oral communications prohibited.

(a) Except as otherwise specifically provided in this subchapter, any person who in the District of Columbia —

(1) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire or oral communication;

(2) willfully discloses or endeavors to disclose to any other person the contents of any wire or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication; or

(3) willfully uses or endeavors to use the contents of any wire or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire or oral communication;

shall be fined not more than \$10,000 or imprisoned not more than five years, or both; except that paragraphs (2) and (3) of this subsection shall not apply to the contents of any wire or oral communication, or evidence derived therefrom, that has become common knowledge or public information.

(b) It shall not be unlawful under this section for —

(1) an operator of a switchboard, or an officer, agent, or employee of a communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication, in the normal course of his employment while engaged in any activity which is a necessary incident to the rendering of his service or to the protection of the rights or property of the carrier of such communication, or to provide information, facilities, or technical assistance to an investigative or law enforcement officer who, under this subchapter, is authorized to intercept a wire or oral communication, but no communication common carrier shall utilize service observing or random monitoring except for mechanical or service quality control checks;

(2) a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication, or where one of the parties to the communication has given prior consent to such interception; or

(3) a person not acting under color of law to intercept a wire or oral communication, where such person is a party to the communication, or where one of the parties to the communication has given prior consent to such interception, unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or

laws of the United States, any State, or the District of Columbia, or for the purpose of committing any other injurious act. (July 29, 1970, 84 Stat. 617, Pub. L. 91-358, title II, § 210(a); 1973 Ed., § 23-542.)

Section references. — This section is referred to in §§ 23-544 and 23-556.

One-party consent must have been given voluntarily in order for interception of wire or oral communication to be admissible as evidence against nonconsenting party. *United States v. Sell*, App. D.C., 487 A.2d 225 (1985), rev'd on other grounds, App. D.C., 525 A.2d 1017 (1987).

Defendant must show improper inducement or coercive threats in order to suppress evidence of wiretap conducted pursuant to one-

party consent under subsection (b)(2). *United States v. Sell*, App. D.C., 487 A.2d 225 (1985), rev'd on other grounds, App. D.C., 525 A.2d 1017 (1987).

Burden of showing voluntary consent under subsection (b)(2) may be met by the government's showing that consenting party engaged in communication knowing that it was being monitored by law enforcement officers. *United States v. Sell*, App. D.C., 487 A.2d 225 (1985), rev'd on other grounds, App. D.C., 525 A.2d 1017 (1987).

§ 23-543. Possession, sale, distribution, manufacture, assembly, and advertising of wire or oral communication intercepting devices prohibited.

(a) Except as otherwise specifically provided in subsection (b) of this section, any person who in the District of Columbia —

- (1) willfully possesses, sells, distributes, manufactures, or assembles an intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication; or
- (2) willfully places in any newspaper, magazine, handbill, or other publication any advertisement of —

(A) any intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication; or

(B) any intercepting device where such advertisement promotes the use of such device for the purpose of the surreptitious interception of a wire or oral communication;

shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

(b) It shall not be unlawful under this section for —

(1) a communication common carrier or an officer, agent, or employee of, or a person under contract with a communication common carrier, in the usual course of the communication common carrier's business; or

(2) a person under contract with the Government of the United States, a State or a political subdivision thereof, or the District of Columbia, or an officer, agent, or employee of the Government of the United States, a State or a political subdivision thereof, or the District of Columbia; to possess, sell, distribute, manufacture or assemble, or advertise any intercepting device, while acting in furtherance of the appropriate activities of the United States, a State or political subdivision thereof, the District of Columbia, or a communication common carrier. (July 29, 1970, 84 Stat. 618, Pub. L. 91-358, title II, § 210(a); 1973 Ed., § 23-543.)

§ 23-552. Government appeals.

In addition to any other right to appeal, the United States or the District of Columbia, as the case may be, shall have the right to appeal from an order granting a motion to suppress made under section 23-551 or from the denial of an application for an order of approval, if the United States or the District of Columbia, as the case may be, shall certify to the judge or other official granting such motion or denying the application that the appeal is not taken for purposes of delay. Appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted. (July 29, 1970, 84 Stat. 625, Pub. L. 91-358, title II, § 210(a); 1973 Ed., § 23-552.)

Section reference. — This section is referred to in § 23-556.

§ 23-553. Authorization for disclosure and use of intercepted wire or oral communications.

(a) Any investigative or law enforcement officer who, by any authorized means and in conformity with this subchapter, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose or use such contents or evidence to the extent that such disclosure or use is appropriate to the proper performance of his official duties.

(b) Any person who, by any authorized means and in conformity with this subchapter, has obtained knowledge of the contents of any wire or oral communication intercepted in accordance with this subchapter, or other lawful authority, or evidence derived therefrom, may disclose the contents of such communication or evidence while giving testimony under oath or affirmation in any criminal trial, hearing, or proceeding before any grand jury or court.

(c) The contents of any wire or oral communication intercepted in conformity with this subchapter, or evidence derived therefrom, may otherwise be disclosed or used only by court order upon a showing of good cause. (July 29, 1970, 84 Stat. 625, Pub. L. 91-358, title II, § 210(a); 1973 Ed., § 23-553.)

Section references. — This section is referred to in §§ 23-548, 23-549 and 23-556.

§ 23-554. Authorization for recovery of civil damages.

(a) Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this subchapter shall —

(1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications; and

(2) be entitled to recover from any such person —

(A) actual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of violation, or \$1,000 whichever is higher;

(B) punitive damages; and

§ 23-555

CRIMINAL PROCEDURE

(C) a reasonable attorney's fee and other litigation costs reasonably incurred.

(b) Good faith reliance on a court order or legislative authorization shall constitute a complete defense to an action brought under this section or any other law.

(c) As used in this section, the term "person" includes the District of Columbia. The District of Columbia shall not assert any governmental immunity to avoid liability under this section. Judgment against the District of Columbia shall not constitute a bar to action against any other person. (July 29, 1970, 84 Stat. 626, Pub. L. 91-358, title II, § 210(a); 1973 Ed., § 23-554.)

Cross reference. — As to return of property by Property Clerk, see § 4-157.

Section reference. — This section is referred to in § 23-556.

§ 23-555. Reports concerning intercepted wire or oral communications.

(a) Within thirty days after the expiration of an order or an extension entered under section 23-547 or 23-548 or the denial of an order of approval, the issuing or denying court shall report to the chief judge of the District of Columbia [Court] of Appeals —

- (1) that an order or extension was applied for;
- (2) the kind of order or extension applied for;
- (3) if the order or extension was granted as applied for, was modified, or was denied;
- (4) the period of the interceptions authorized by the order, and the number and duration of any extensions of the order;
- (5) the offense specified in the order or application, or extension of an order;
- (6) the identity of the applying investigative or law enforcement officer, the agency making the application, and the person authorizing the application; and
- (7) the character and location of the facilities from which and the place where communications were (and were to be) intercepted.

(b) In January of each year the United States Attorney for the District of Columbia shall report to the Congress of the United States and the chief judge of the District of Columbia Court of Appeals —

- (1) the information required by paragraphs (1) through (7) of subsection (a) of this section with respect to each application for an order or extension made during the immediately preceding calendar year;
- (2) a general description of the interceptions made under such order or extension, including —

(A) the approximate character and frequency of incriminating communications intercepted;

(B) the approximate character and frequency of other communications intercepted;

(C) the approximate number of persons whose communications were intercepted; and

E FEDERAL PAGE

the new aeronautics
in order of impor-

technology for a super-
referred to as High
Transport (HSCT)—
year 2005 could fly at
ching 1,500 mph.

"must be and will be
environment, it will
the ozone layer, and it
noise regulations,"
An inability to meet
killed the SST effort
He said "son of SST"
ore economical suc-
nefficient Concorde.
program is intended,
o develop a ceramic
terial for use in the
tem that can operate
s at temperatures
egrees Fahrenheit.
ke possible the high-
combustion required
almost all ozone-de-
ons in the exhaust.

ch also will focus on
technologies such
aut nozzles, intend-
te the 120-decibel
ated with the Con-

high-payoff technol-
for the commercial
n, such as more eco-
eight structural ma-
efficient aircraft en-
avigation systems
ways of detecting
and other safety
aging U.S. commer-
t.

national resources,
l to as "infrastruc-
s high-performance
d wind tunnels to
est the new technol-
ie of deterioration in
tunnels "sneaked up
s said, noting that
in recent times has
o use European fa-
have surpassed us,"

search jointly with
epartment for a hy-
national Aerospace
ble successor to the
the craft would take
e an airplane and fly
the speed of sound.
hurt the cause that
aeronautics activity
ed by NASA's Lewis
ter in Cleveland,
to be in the district
s Stokes (D-Ohio),
of the House Appro-
committee that funds

3rd Security Review Is Out of Shadows

Administration Presses Overhaul of Cold War-Era Secrecy Rules

By R. Jeffrey Smith
Washington Post Staff Writer

Excessive secrecy has suddenly become a hot topic in the Clinton administration, which yesterday announced the start of a third major review of Cold War-era rules that govern creation of "classified" information.

Vice President Gore described the new review of security practices and procedures at the Defense Department and the CIA as an effort to "get rid of unnecessary bureaucracy, identify significant savings and improve efficiency" in the government's massive effort to shield information from public or foreign disclosure.

The review comes on top of a government-wide review of secrecy that President Clinton ordered last month and another review of contractor secrecy being conducted by the director of the Defense Security Programs office, a circumstance that provoked one critic to wonder if the streamlining effort was simply enlarging the bureaucracy.

But the number of secrecy reviews may be related to the magnitude of the problem. According to official estimates, the government last year took 6.3 million classification actions, creating an estimated 19 million pages of information that only selected government officials can see.

No one has a reliable estimate of the total number of classified documents, but Steven Aftergood of the Federation of American Scientists has learned that several still-classified documents date from before World War I and he estimated the total at "hundreds of millions if not billions."

Supporting this mountain of restricted information are hundreds of elaborate secrecy rules and regulations, involving costs estimated by the CIA in the billions of dollars.

An internal memorandum outlining the charter for the new review states that "the current security system is fragmented, complex, and costly" and that "a new approach... is necessary." It said the review should encompass CIA and Defense Department procedures for safe-



R. JAMES WOOLSEY
... committed to curtailing secrecy

guarding sources, documents, facilities, computer systems, personnel, operations and policymaking, as well as information exchanges with foreign governments.

The review is to be conducted by a 10-member committee chaired by

According to official estimates, the government last year created some 19 million pages of information that only selected officials can see.

Washington attorney Jeffrey H. Smith, a former Senate Armed Services Committee staff member who directed the Clinton administration's transition team at the Pentagon. Seven other members of the panel are former CIA, Defense or National Security Agency officials,

while two represent major defense contractors.

The group's final report, due next February, will be unclassified, according to CIA spokesman Peter Earnest. But the committee charter states that all the group's meetings are exempt from a federal law permitting public attendance.

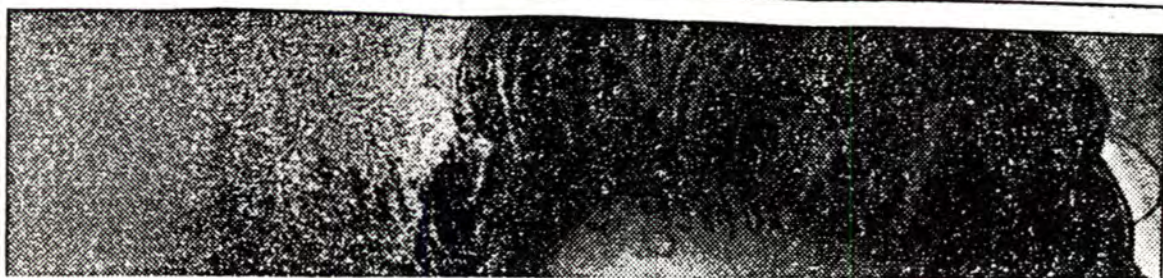
Aftergood said he is concerned that the new review "is duplicative of existing efforts... and will dilute authority" among the competing groups, lessening the chance that their recommendations will be implemented. The review ordered by Clinton, for example, is chaired by Steven Garfinkel of the Information Security Oversight Office in the General Services Administration. It encompasses not only the Defense Department and CIA, but the Energy Department and other agencies that churn out truckloads of official secrets.

The aim of Garfinkel's review, according to a copy of Clinton's order, is to answer such questions as: "what steps can be taken to avoid excessive classification... to declassify information as quickly as possible" and to reduce the number of "special access" programs, a category of military and intelligence endeavors that are considered so sensitive their existence is sometimes never acknowledged.

Aftergood is concerned that "instead of streamlining and consolidating, the reviews will produce chaos." But CIA spokesman Earnest said their recommendations will be coordinated, and that the group appointed yesterday "will serve as an outside check" on what the CIA and Defense Department are doing in conjunction with the government-wide review.

Some independent experts speculated that the new group was created in part to ensure that the CIA and Defense Department will play a major role in the secrecy debate, possibly fending off excessive recommendations for openness.

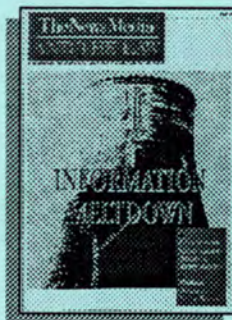
But Earnest said CIA Director R. James Woolsey and Defense Secretary Les Aspin are strongly committed to curtailing excessive secrecy. He added, "The proof of the pudding is in the tasting. Let's judge it by its results."



ate spending patterns
Senate spenders
House spending patterns
House spenders
races

PUBLICATIONS

The News Media and The Law is the Reporters Committee's quarterly magazine, which provides complete summaries of recent cases affecting the news media. **\$25 per year**



How to Use the Federal FOI Act explains your rights under the federal Freedom of Information and Privacy acts and explains how to request information and to appeal its denial. Includes sample letters. **\$3**



Updated 3rd Edition

The First Amendment Handbook is a pocket guide to assist reporters and editors in dealing with a variety of everyday legal problems, including restrictions on the use of hidden recorders, access to courts and other places, protecting confidential sources and information, libel, invasion of privacy, censorship and copyright. **\$4**



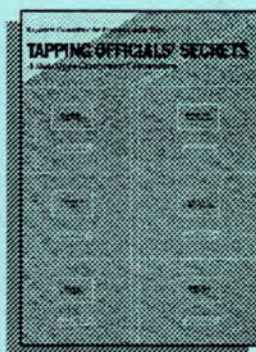
Access to Electronic Records analyzes state laws and decisions concerning government information stored in computers and strategies for obtaining access to data in electronic form. **\$5**



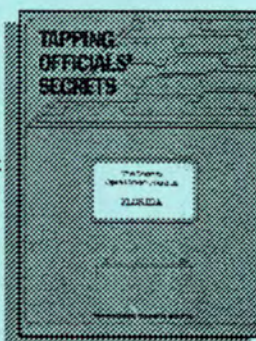
Access to Police Records is a comprehensive, 50-state and D.C. survey of the availability of information from law enforcement. The guide provides references to statutes as well as case law. **\$2**



Tapping Officials' Secrets: A State Open Government Compendium is a comprehensive guide to using state open records and meetings laws in all states and the District of Columbia. **\$325**



Tapping Officials' Secrets is available for each state. Each booklet provides the same information included in the compendium but at a modest cost for those who need to know about the law in their state or neighboring jurisdictions. **\$8.00 each**



Updated Second Edition Now Available:

Just Released:

Access to Places is an overview to the laws that govern access to public and private property as well as crime scenes, and includes suggestions for minimizing restrictions on access to crimes, accidents and disasters. **\$2**



Agents of Discovery is a continuing report on the incidence of subpoenas served on the news media, summarizing the results of a nationwide survey of newspapers and TV stations. **\$3**



ALSO AVAILABLE:

- **Access to Juvenile Courts** \$2
- **Access to the Legislature** \$2
- **Cameras & Microphones in Public Meetings** \$2
- **Confidential Sources & Information** \$2
- **Judicial Records** \$2
- **Photographers' Guide to Privacy** \$2
- **The Bush Administration and the News Media** \$5

THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS

1735 EYE STREET, NW • SUITE 504 • WASHINGTON, DC 20006

(202) 466-6313

QTY.	PUBLICATION	PRICE	SHIPPING PER COPY	TOTAL
	<i>Tapping Officials' Secrets: A State Open Government Compendium [complete 50-state & D.C. set] 2nd Edition</i>	\$325.00	CALL FOR COST	
	<i>Tapping Officials' Secrets: The Door to Open Government in</i>			
	STATE _____	8.00	\$2.50	
	STATE _____	8.00	2.50	
	STATE _____	8.00	2.50	
	<i>Access to Electronic Records</i>	5.00	1.00	
	<i>The Bush Administration and the News Media</i>	5.00	--	
	<i>First Amendment Handbook (3rd edition, 1992)</i>	4.00	.75	
	<i>How to Use the Federal FOI Act</i>	3.00	1.00	
	<i>Agents of Discovery: A Report on the Incidence of Subpoenas Served on the News Media (specify either 1991 or 1993 report)</i>	3.00	.75	
	<i>Access to Juvenile Courts</i>	2.00	.50	
	<i>Access to the Legislature</i>	2.00	.50	
	<i>Access to Places</i>	2.00	.50	
	<i>Cameras & Microphones in Public Meetings</i>	2.00	.50	
	<i>Confidential Sources & Information</i>	2.00	.50	
	<i>Judicial Records: A Guide to Access in State & Federal Courts</i>	2.00	.50	
	<i>Photographers' Guide to Privacy</i>	2.00	.50	
	<i>Police Records: A Guide to Effective Access in the 50 States & D.C.</i>	2.00	.50	
GRAND TOTAL				

I would like to contribute to the Reporters Committee.

- ☐ \$25: I will receive a one-year subscription to the quarterly magazine *The News Media and The Law*.
- ☐ \$40: I will receive *The News Media and The Law* and *The First Amendment Handbook*.
- ☐ \$100: *The News Media and The Law*, *The First Amendment Handbook* and a one-year subscription to *Publishers' Auxiliary* (incorporating *News Media Update*).
- ☐ Other: _____



NAME _____

ORGANIZATION _____

STREET ADDRESS _____

CITY _____

STATE _____

ZIP _____

TOTAL AMOUNT ENCLOSED _____

YOUR CONTRIBUTION IS TAX-DEDUCTIBLE TO THE EXTENT PERMITTED BY LAW.

JOINT SECURITY COMMISSION

- TAB A Joint Security Commission Charter
- TAB B Terms of Reference
- TAB C Vice Presidentail Statement Announcing
Establishment of Joint Security Commission
- TAB D Questions and Answers
- TAB E Commissioners

OFFICE OF THE DIRECTOR OF CENTRAL INTELLIGENCE
OFFICE OF THE SECRETARY OF DEFENSE

1. ESTABLISHMENT. Pursuant to the provisions of the National Security Act of 1947 and Executive Order 12333, the Director of Central Intelligence (the DCI) and the Secretary of Defense (the Secretary) hereby approve the establishment of the Joint Security Commission (the Commission). The Commission shall be established by the Director of the Central Intelligence Agency and shall be exempt from the provisions of the Federal Advisory Committee Act in accordance with Section 4(b)(1) of Public Law 92-463.
2. MEMBERSHIP AND ORGANIZATION. The Commission will consist of nine members including the chairman selected jointly by the Secretary and the DCI. Members will serve as part-time advisory personnel under section 303 of the National Security Act. Members serve at the pleasure of the DCI and the Secretary. The chair may establish committees and task groups from the membership for the purpose of carrying out its mission.
3. DUTIES. By 1 February 1994, the Commission shall conduct a comprehensive review of the security practices and procedures under the authorities of the DCI and the Secretary and shall present to the DCI and the Secretary its recommendations and implementing actions to improve such security practices and procedures. From February 1 to June 1, 1994, the Commission shall monitor implementation of decisions by the DCI and the Secretary made pursuant to its recommendations.
4. RELATIONSHIP WITH OTHER ACTIVITIES. The Commission will have full access to all security compartments, programs, and data it may require from the defense and intelligence communities. It will have the full support and cooperation of all agencies and components.
5. ADMINISTRATIVE PROVISIONS. The Commission will meet at the call of the chair. The Commission will be assisted by an Executive Secretary and a Deputy Executive Secretary and a small staff from within the Department of Defense and the intelligence community. The security elements of the

Department of Defense, the Central Intelligence Agency and other intelligence community organizations will assist the Commission in its work. The CIA will provide administrative support to the Commission.

6. DURATION. The Commission shall terminate by June 1, 1994.

Director of Central Intelligence

Secretary of Defense

TERMS OF REFERENCE

One of our government's fundamental challenges today is to balance the need for an effective flow of information with the need to protect the safety and privacy of people and the confidentiality and integrity of valuable information. The success of our nation in a world of rapid technological change depends more than ever on our unsurpassed ability to exploit the open exchange of information. In a period in which fiscal resources are scarce and whole new systems of communications and information are emerging, we must rethink the assumptions behind our security practices to ensure that we are taking a sound and cost effective approach.

A new approach to security is necessary. Security policies should be reoriented based on reasonable risk management rather than near absolute risk avoidance. The current security system is fragmented, complex and costly. Our charge is to assure the adequacy of protection, within the contours of a security system that is simplified, more uniform and more cost effective.

- In performing the duties assigned by the Director of Central Intelligence and the Secretary of Defense, the Joint Security Commission shall examine all aspects of security practices and procedures within the Department of Defense and the Intelligence Community, including threat analysis, classification, information systems, personnel, physical, technical, operations, industrial, international and related security domains. All compartmented and collateral security programs will be included.

- Among the factors the Commission shall take into account are the need for an effective flow of information and for compatibility between military and commercial technologies; the relationship between threat assessments and security programs; the emergence of new systems of communications and information; the soundness and cost-effectiveness of security practices; new security countermeasures methods and technologies; and fiscal constraints.

- The Commission shall consider various security issues such as identification of data, activities and people needing special protection in the context of risk management; protection of intelligence sources and methods; security for Special Access Programs; foreign access to sensitive industries, facilities and information; exchanges and

relationships with other nations and international entities; the involvement of policymakers, commanders and other users in security policy formulation, execution and resource management; and exchange of personnel and information across government, industry, and academia.

- The Commission shall examine classification, declassification, compartmentation and other controls; protection of information assets in documentary and electronic form; measures to provide for confidentiality, integrity, and availability; the impact of security procedures on the timeliness, accessibility and usefulness of sensitive information to consumers; and related information security matters.

- The Commission shall examine personnel security programs, including investigations, adjudications, and appeals; Special Access determinations; use of the polygraph; and establishment of common counterintelligence and security data bases.

- The Commission shall examine requirements for physical and technical security of facilities, equipment, and information, as well as for protection of personnel and infrastructure against terrorist and criminal activity.

- The Commission also shall examine cross-discipline management; career paths and inter-agency assignments, training; research and development; the practices and procedures for providing intelligence, counterintelligence, and law enforcement information to policymakers, commanders and other users; procedures that link security measures and costs to threat assessments and risks of disclosure; and related matters.

- The Commission shall determine that all implementing actions are taken promptly by appropriate entities and shall regularly advise the DCI and the Secretary on the status of all implementing actions.

VICE PRESIDENTIAL STATEMENT ANNOUNCING ESTABLISHMENT
OF JOINT SECURITY COMMISSION

The President and I are pleased to announce the establishment of a Joint Security Commission by the Director of Central Intelligence and the Secretary of Defense. The Commission will conduct a comprehensive review of the security practices and procedures of the intelligence and defense communities and report their findings to Secretary Aspin and Director Woolsey. The Commission members are: Jeffrey Smith, Chair; Duane Andrews, Robert Burnett, Ann Caracristi, Antonia Chayes, Anthony Lapham, Richard Stolz, Harry Volz, and General Larry Welch, USAF (Ret.).

One of our government's fundamental challenges today is to balance the need for an effective flow of information with the need to protect the confidentiality, integrity, and availability of valuable information. It is vital that the Intelligence Community's information be made available as rapidly and widely as possible, consistent with necessary security constraints. The goal of achieving greater compatibility between our military and civilian industrial sectors through dual-use technologies also requires an examination of security policies and procedures. In a period of diminishing resources and the emergence of new systems of communications and information management we must rethink the assumptions behind security practices to ensure that we are taking a cost-effective approach while protecting our national interest.

Therefore, the President and I look to the Secretary and the DCI, with the assistance of the Joint Security Commission, for initiatives that will help the intelligence and defense communities contribute more effectively to the achievement of national objectives. Because the intelligence and defense communities produce the greatest amount of classified and sensitive information and incur the largest security costs, the Joint Security Commission's work will be a valuable gauge by which to look at government-wide security programs.

I expect the cooperation of all Department and Agency heads with the Joint Security Commission as established by the Director of Central Intelligence and the Secretary of Defense.

VICE PRESIDENTIAL STATEMENT ANNOUNCING ESTABLISHMENT
OF JOINT SECURITY COMMISSION
QUESTIONS AND ANSWERS

QUESTION: What are the objectives of the Joint Security Commission?

ANSWER: The commission will examine all aspects of security practices and procedures within the Department of Defense and the Intelligence Community. Factors the commission will consider are:

- The need for an effective flow of information and for compatibility between military and commercial technologies;
- The linkage between threat assessments and security programs;
- The emergence of new communications and information systems;
- The soundness and cost effectiveness of security practices;
- New security countermeasures methods and technologies;
- Fiscal constraints.

QUESTION: What was the impetus for establishing the Joint Security Commission?

ANSWER: The decision grew out of a management review task force commissioned by the Director of Central Intelligence last October which included representatives from the Department of Defense. It examined policy, management, and structural changes that would make substantial improvements in the infrastructure of the Intelligence Community. In the judgment of the task force, the greatest deterrents to major savings in infrastructure are current security policies and practices. The DCI and the Secretary of Defense were persuaded by these findings to establish a Joint Security Commission to help us rethink the assumptions behind our security practices to ensure that we are taking a sound, cost-effective approach.

QUESTION: What are the anticipated cost savings?

ANSWER: We have not set targets but believe there is the potential for significant savings. That's one purpose of the commission.

QUESTION: Why is this effort focused on the Department of Defense and the Intelligence Community?

ANSWER: The intelligence and defense communities produce the greatest amount of classified and sensitive information and incur the greatest security costs.

QUESTION: When will the Joint Security Commission complete its work?

ANSWER: By February 1, 1994, the Commission will present to the Secretary of Defense and the DCI its recommendations and implementing actions. From February to June 1, 1994, the Commission will monitor decisions by the DCI and Secretary of Defense relative to these recommendations.

QUESTION: Will the Commission consider revision of the Executive Order on classified information?

ANSWER: The Administration has begun a separate, governmentwide effort to consider revisions of the Executive Order on classified information. It is being led by the Director, Information Security Oversight Office, and will be coordinated with the Joint Security Commission.

QUESTION: Will the Joint Security Commission report be classified?

ANSWER: That will be decided by the Commission. However, we are predisposed to make as much of it as possible unclassified.

QUESTION: Who are the members of the Commission?

Jeffery Smith
Duane Andrews
J.R. Burnett
Ann Caracristi
Antonia Chayes
Anthony Lapham
Richard Stolz
Harry Volz
General Larry Welch, USAF (Retired)

COMMISSIONERS

Jeffrey Smith - is a partner in the law firm of Arnold and Porter who served as Chief of the Clinton Transition Team at the Department of Defense. He is a former General Counsel of the Senate Armed Services Committee and was Senator Nunn's designee on the Iran/Contra Committee and the Senate Select Committee on Intelligence. Mr. Smith previously served as the Assistant Legal Adviser for Law Enforcement and Intelligence in the Department of State and earlier, as an Army JAG officer, as the Pentagon's lawyer for the Panama Canal negotiations.

Duane Andrews - is senior vice president for C4 and Information Systems, Science Applications International Corporation. Mr. Andrews has held positions as the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, and as a professional staff member with the House Permanent Select Committee on Intelligence.

J.R. Burnett - is the chairman of the Strategic Advisory Group for the U.S. Strategic Command, and the Scientific Advisory Board of the National Security Agency. He retired as executive vice president and deputy general manager of TRW's Space and Defense Sector after thirty-five years of service with the company. He is a member of a number of government committees, panels and corporate boards of directors.

Ann Caracristi - is a consultant to the NSA Scientific Advisory Board and a member of the Board of Visitors of the Defense Language Institute Foreign Language Center. She is a former Deputy Director of the National Security Agency, served two terms as President of the Association of Former Intelligence Officers, and was a member of the Chief of Naval Operations Executive Panel from 1982 to 1991.

Antonia Handler Chayes - is a Senior Consultant at ENDISPUTE, Inc., where she serves as mediator and arbitrator in business disputes. During the Carter Administration she was Under Secretary of the U.S. Air Force and also served as Assistant Secretary of the Air Force for Manpower, Reserve Affairs and Installations. Ms. Chayes is a director of United Technologies Corporation, an Adjunct Lecturer at the Kennedy School of Government and has been an Adjunct Professor at the Georgetown School of Law. She is a member of the Aspen Institute Core Group on Strategy and Arms Control, and of the Dartmouth Conference of the Kettering Foundation.

Anthony Lapham - is a partner with the law firm of Shea and Gardner. He is a former CIA General Counsel and member of the President's Intelligence Oversight Board.

Richard Stolz - served with the CIA for thirty-four years, most recently as the Deputy Director for Operations. He is the recipient of numerous awards in the field of intelligence, including the National Security Medal for distinguished achievement in the field of intelligence relating to the national security.

Harry Volz - is Director of Corporate Security, the Grumman Corporation. Mr. Volz currently serves as co-chair of the National Industrial Security Program Steering Committee and has held prominent positions on industry-wide security committees during his more than thirty years of corporate security experience.

General Larry Welch USAF (Retired) - is the President and Chief Executive Officer of the Institute for Defense Analysis. General Welch was the former Chief of Staff, USAF, Commander in Chief, Strategic Air Command and Vice Chief of Staff, USAF. He is currently a consultant to the Defense Science Board and active in numerous national security associations.