

MARINE CORPS DOT FBI CIA NARA FEMA
DOJ TREASURY ARMY STATE AIR FORCE

PRD 29



TASK FORCE

DIA COAST GUARD OPM NAVY DIS NRC CCISMO
COMMERCE DOE NSA DOD SI OSD OMB



Information Security Oversight Office
750 17th Street, NW., Suite 530
Washington, DC 20006

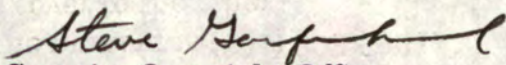


August 11, 1993

MEMORANDUM FOR: The Honorable
John Podesta
Assistant to the President and Staff Secretary

The Honorable
George Tenet
Special Assistant to the President and
Senior Adviser for Intelligence Programs

Michael Waguespack
Director for Counterintelligence Programs
National Security Council

FROM: Steven Garfinkel 
Director, Information Security Oversight Office

SUBJECT: Department of Energy Declassification Briefing

The Secretary of Energy has cited the declassification of information, especially that related to environmental health and safety, as a major initiative in DOE's reinventing Government program. Yesterday, A. Bryan Siebert, Director of DOE's Office of Classification, briefed ISOO on this initiative. Because the bulk of DOE's classified information is "born classified" as Restricted Data (RD) or Formerly Restricted Data (FRD) under the Atomic Energy Act, DOE's initiative is largely outside the scope of our efforts to rewrite the Executive order on national security information. Nevertheless, the parallel goals and objectives are striking, and DOE's proposed methodology is very informative. For example, to achieve all of their proposed objectives would require legislation to amend the Atomic Energy Act to abolish the concept of "born classified."

One or more of you may be interested in receiving a similar briefing from Mr. Siebert or his supervisors. His telephone number is (301) 903-3521. I've sent the same memorandum under separate cover to the other addressees.

MEMO

To: John Podesta
From: Gideon Stein
Date: August 13, 1993
Re: Declassification Policy

In a discussion with Harold Relyea of the Congressional Research Service he provided information on the extent to which the National Archive is declassifying information without the benefit of public inquiry. According to Mr. Relyea there currently is no effective policy for declassification. He said that the Archives has been dragging its heels on declassification and thus has been subject to criticism from Congress. With budgets tight and the relative high costs associated with declassification, the neither the Nation Archives nor the Information Security Oversight Office have been very proactive in declassifying and disseminating information.

The Presidential Review Directive 29 addresses some of the problems related to the lag in declassification. PRD 29 proposes both a systematic and a mandatory review for declassifying documents. The **systematic declassification review** would cover agencies with classified information under the Executive Order 12356.

- It applies to pertinent records no later than 25 years from the date of creation.
- Agencies should prioritize the systematic review of researcher interest and the possibility of declassification upon review.

The Archivist of the United States is charged with conducting a systematic declassification review program for national security protection information in the National Archive beginning when the Order takes effect.

- This applies to pertinent records no later than 25 years from the date of their creation.
- The Archivist shall prioritize the systematic review of these records depending upon the degree of researcher interest and the potential for declassification upon review.
- Records shall be reviewed in accordance with the standards of the Order.
- The Director of ISOO shall make sure that agencies provide the Archivist with adequate and current declassification guides.

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

Mandatory Declassification Review

All information classified under this Order or its predecessor is subject to a review for declassification by the originating agency if:

- The request is made by a US citizen or permanent resident alien, a federal agency, or a state or local government.
- The request describes the document or material containing the information with enough specifics to enable the agency to locate it with a reasonable amount of effort.
- The information has not been reviewed for declassification within the past two years.

The following are exceptions to the above provision.

- Information originated by a President, the White House staff, by committee, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President.

The Archivist of the US shall have the authority to review, downgrade and declassify information under his control pursuant to sections 2107, 2111, 2111 note or 2203 of title 44 US Code.

- Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with applicable laws that pertain to the respective presidential papers or records.
- Any decision by the Archivist may be appealed to the Director of ISOO.
- Agencies with primary subject matter interest shall be notified of the Director's decision on such appeals and may further appeal to the NSC.
- The information shall remain classified pending a prompt decision on the appeal.

Agencies conducting a mandatory review for declassification shall do so with information no longer required for protection under this Order. The information shall be released unless withholding it is otherwise authorized and necessary under law.

Agency heads shall develop procedures to process requests for the mandatory review of national security protected information.

- This applies to information classified under this or previous Orders.

- They should provide a means for appealing a denial of a mandatory review request.

The Secretary of Defense shall develop special procedures for reviewing cryptologic information.

- The DCI should do the same for reviewing information pertaining to intelligence activities, sources, or methods.
- The Archivist shall develop special procedures for the review of information in the National Archives of the United States.



The National Security Archive

Documenting U.S. Foreign Policy

A Project of the Fund for Peace

FAX COVER SHEET

To: John Podesta / Gideon Stein
From: Sheryl Walter
Date: 8/4/93
Number of pages in addition to cover sheet: 9

If there is a problem with this transmission, please call us at 202-797-0882 as soon as possible.

National Security Archive
1755 Massachusetts Avenue NW #500
Washington, DC 20036
Telephone: 202-797-0882
Fax: 202-387-6315



The National Security Archive

Documenting U.S. Foreign Policy

A Project of the Fund for Peace

August 4, 1993

VIA FAX: 456-2215

TO: John Podesta
Gideon Stein

FROM: Sheryl Walter

RE: Briefing materials on needed revisions to E.O. 12356

Per Gideon's request this afternoon, accompanying this memo are briefing materials we have prepared on needed changes to the Reagan executive order governing security classification.

Included are a three-page discussion paper I prepared with Steve Aftergood from the Federation of American Scientists and the executive summaries of testimony by National Security Archive staff at the public hearings held by ISOO on June 9 and 10.

If you have any questions or need additional information, or if we may provide any other assistance, please do not hesitate to give us a call.



The National Security Archive

Documenting U.S. Foreign Policy

A Project of the Fund for Peace

PRESIDENTIAL REVIEW DIRECTIVE ON CLASSIFICATION

Discussion Paper May 14, 1993

(Revised May 21, 1993)

The Presidential Review Directive signed by President Clinton on April 26, 1993 sets out a series of questions for the task force the directive establishes, headed by Steve Garfinkel of the Information Security Oversight Office (who also headed the office during the Reagan/Bush years), to address in preparing a new draft executive order on classification by November 30. The directive's questions, which overlap to a large extent, are set out below, with some suggested initial responses listed below. Other approaches and suggestions are welcome.

1. 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?

In principle, nothing should be automatically classified merely by virtue of its "type". As President Clinton has stated, "Government information is a public asset," and thus belongs to the American people and not government officials. However, some information could genuinely cause identifiable damage to the national security. The following types of information are suggested as categories *eligible* for classification (but not to be automatically classified absent a showing of identifiable damage from release):

- Details of advanced weapons system design and operation (but not including the existence or costs of weapons programs).
- Details of pending military operations.
- Details of ongoing diplomatic negotiations.
- Identities of confidential intelligence sources that could be jeopardized by disclosure; current cryptographic methods in intelligence; and operations characteristics of advanced intelligence technologies.
- Change references in the current executive order from "foreign government information" to "foreign government documents."
- Change references in the current executive order from "national security" to "national defense."
- Change references in the current executive order from "foreign relations" to "foreign policy."
- Add a public interest balancing test for release of information.
- Abolish the ability to reclassify information already in the public domain, which the Reagan order for the first time allowed.

2. What steps can be taken to declassify information as quickly as possible?

Return to the practice of automatic declassification with sunset dates, as promulgated by President Nixon in E.O. 11652 and President Carter in E.O. 12065, by which most documents would be automatically declassified after the passage of some sensible period of time. (The period of automatic declassification was ten years under Nixon, six years under Carter. However, the national security bureaucracy largely ignored this instruction, and compliance will therefore require a suitable enforcement mechanism.)

To eliminate the wasteful, time-consuming practice of independent multi-agency declassification review of many documents, establish a form of "universal on-site declassification authority" so that declassification may be executed by a single review at a single agency. In other words, the agency in possession of a document, even if it is not the originating agency, should be able to declassify it without serial referrals to multiple agencies, which often lengthens by years the time before an agency record is publicly available. This step alone would dramatically shorten the time needed to declassify many documents.

3. 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?

It is essential that older documents be declassified in bulk without painstaking and extraordinarily expensive individual page-by-page review conducted by multiple reviewers. No one today attempts to defend the continued classification of some documents from World War I, for example, yet resources have not been sufficient to win their releases through the current individual declassification review process.

With a few exceptions, all classified documents older than 20 years should have their classification cancelled. Historians have used as a cancellation period 30 years; the former head of the National Archives says 40 years; former CIA director Robert Gates proposed a 10 year date for declassification of National Intelligence Estimates; Edward Teller, a father of the ~~atom~~ ^{hydrogen} bomb, says one year. In addition, all archival indices, catalogues, and finding guides to government documents should be declassified immediately.

4. What steps can be taken to reduce the number of, and to provide adequate oversight and control over, special access programs?

When the "need to know" requirement is properly enforced, "special access" becomes unnecessary. Special access (or "black") programs are the most highly

classified programs, and the most subject to abuse. In many cases, their very existence is a secret. They include weapons acquisition programs, intelligence programs, and military operations.

As a first step, all weapons acquisition programs, which have proven to be a most problematic category, should be removed from special access status. In the

post Cold War era, there is no justification for concealing the existence of a new aircraft, tank, or submarine program. If it is possible to achieve a regular classification system that has credibility, the special access system can be eliminated altogether with no loss of security.

5. 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?

To gain access to classified information, one currently must not only have a security clearance, but also a "need to know" the specific information in question. As a consequence of the diminished credibility of the classification system, the need to know principle has been commonly disregarded. (And many of the most damaging espionage cases of recent years involved persons who were both properly cleared and had a "need to know".) This is primarily an internal educational and management issue. But if fewer documents are improperly or unnecessarily classified, respect for the system will grow and compliance with the "need to know" principle increase.

Broad distribution of classified information also complicates the declassification process, often leading to multiple declassification reviews of the same document. Establishing centralized indices of declassified documents should be considered to address this problem.

6. What steps can be taken to increase individual accountability for the operation of the classification system?

Original classifiers should be identified on all documents, with a citation of the individual's basis for classification of the document. Individuals who habitually overclassify, even if good faith, should have their classification authority revoked.

An additional significant problem that needs to be addressed is the procedure under which this review is taking place. Entrenched civil servants have been put in charge of the process and no ongoing formal means for public input appears to be contemplated. On May 20, ISOO published a notice in the Federal Register of two days of public "hearings" on June 9 and 10 at which interested parties may make presentations to the seven subcommittees set up to conduct this review. A deadline for written submissions is set for July 14. No further formal public input appears contemplated, nor any public notice and comment procedures before the new draft order is submitted to the NSC.

Sheryl Walter, National Security Archive
Steve Aftergood, Fed. of Am. Scientists

The National Security Archive

Documenting U.S. Foreign Policy

A Project of the Fund for Peace

ISOO Hearings: Changes to the Security Classification System

Committee on Classification Standards -- June 9, 1993,

Testimony of Sheryl L. Walter, General Counsel

I. Introduction

II. Comments on the Committee's Scope of Review

A. Questions and Answers --

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

A: Far fewer.

Q: Do we need three levels of classification?

A: Not the right question to solve the problem.

B. The ISOO proposal before you -- where in the executive order you should list the current standard is not this committee's fundamental problem to solve. You need to establish overarching workable principles upon which classification decisions can rest. Threats exist in a post Cold War world, but an effective and credible classification system must be able to identify those threats in more specific terms than was done during Cold War.

III. Recommendations

A. Establish as the core standard for classification standards a requirement that there be identifiable damage from release. See the Supreme Court's decision in Dept. of Justice v. Landano (copy attached) (requiring as showings of identifiable harm through "fairness, public policy, probabilities, and common sense" as a precondition to secrecy).

B. Balance identifiable harm findings against the public's interest in disclosure.

C. Apply the concept of risk management, not risk avoidance, and incorporate real cost-benefit calculations of secrecy.

D. Any categories must be narrow and reasonably related to the ability to identify damage in a particularized sense. Examples of narrow categories include:
 National defense and pending military ops (not national security)
 Ongoing diplomatic negotiations (not foreign relations)
 Foreign government documents (not foreign government information)
 Identifiable damage to a source
 Weapons technology/specifications (not the fact or cost of programs)

IV. Conclusion -- This committee's report, and the draft order that follows, must:

A. Incorporate a risk management, not risk avoidance approach.

B. Create a credible system that protects what needs protection, but no more.

C. Create a system that we can afford.

D. Makes it harder to classify than not to classify.

E. Takes into account the fact that government information belongs to the people.

The National Security Archive

Documenting U.S. Foreign Policy

A Project of the Fund for Peace

ISOO Hearings: Changes to the Security Classification System
Committee on Excessive Classification -- June 9, 1993,
Testimony of Lynda Davis, FOIA Coordinator, Sheryl L. Walter, General Counsel

I. Introduction

II. Problem Discussion

A. Overclassification is a universally recognized problem that concerns those inside and outside the government.

B. The National Security Archive's experience with excessive classification by agencies shows:

1. No cost-benefit analysis
2. No examples of release of information harmful to national security; but many examples of overclassification

III. Recommendations

A. Prohibit the reclassification of information

B. Weigh the costs and benefits of classifying information by balancing the public-interest benefit from release with identifiable harm to the nation

C. Give every secret a sunset, or automatic, release date no more than ten years from creation, written on the document

D. Reduce the number of departments and original classifiers of information

E. Set specific timetables for automatic declassification of documents

F. Identify by name the original classifiers on all documents

G. Give declassification of information the same or greater emphasis accorded to classification

H. Provide incentives for challenging improper classification decisions

I. Create narrow and specific categories of information eligible for classification (e.g. change references in the current executive order:
* from "foreign government information" to "foreign government documents"
* from "national security" to "national defense"
* from "foreign relations" to "foreign policy."

The National Security Archive

Documenting U.S. Foreign Policy

A Project of the Fund for Peace

Recommendations to the Committee on Oversight of the PRD 29 Task Force

June 9, 1993

By Thomas S. Blanton, Executive Director
The National Security Archive

OVERVIEW:

- The end of the Cold War demands a paradigm shift in the secrecy system, and there is an emerging consensus on the need for radical change and far fewer secrets.
- The primary conceptual shift is one that moves from a system of maximum risk avoidance to a system of reasonable risk management, precisely because the former system is so costly and the risks in the post-Cold War world are so much smaller.
- Reasonable risk management should include a public interest balancing test and a cost-benefit analysis for every secret.

RECOMMENDATIONS FOR OVERSIGHT:

Special Access Programs:

- Two-year sunset on SAP's, since, by definition, these are fairly impervious to oversight.
- Remove weapons acquisition programs from SAP's.
- Establish a long-term goal of abolition of SAP's.
- Incentives for employees to challenge need for SAP's.

Individual Accountability:

- Name of classifier on each secret, along with justification. (Name, not position, because the latter simply builds in the institutional commitment to the secret.)
- Sunset on every secret. (Agency heads can extend sunsets on very limited groups of secrets, but only after a balancing test and a cost-benefit analysis).
- Incentives for employees to challenge classifications.
- Performance plans and individual performance annual reviews should include openness and declassification as criteria for success and promotion, not simply classification management.

Oversight:

- By agencies and ISOO: Annual report to relevant Congressional committees on all SAP's showing progress on long-term goal of eliminating SAP's.
- By ISOO: Delegate to ISOO analysts ability to oversee SAP's.
- By Congress: The classification system needs a statutory mandate, with Congressional hearings and passage of law.
- By agencies: Create a zero-based secrecy budgeting system, which means tasking each agency to identify, by time period, its most sensitive materials. All other materials move into automatic declassification process.
- By outside experts: Establish an independent review board for Cold War documents, to create criteria for bulk declassification and oversee its implementation.
- By taxpayers: Establish agreed-upon cost measurement methodology for cost of keeping secrets, and publish this and use it for cost-benefit analyses on individual classification decisions.



The National Security Archive

Documenting U.S. Foreign Policy

A Project of the Fund for Peace

RECOMMENDATIONS FOR ISOO PANEL ON DECLASSIFICATION

Malcolm Byrne

June 10, 1993

1. Mandate bulk declassification after 20 years, allowing for a small number of precisely defined exceptions for information that would either cause identifiable harm to the national defense or risk lives.
2. Establish an outside independent review board, comprised predominantly of archivists, historians and others who use the information, but including representatives who have worked as original classifiers (but are now outside the government), to formulate those limited criteria for withholding information.
3. Once precise guidelines have been set, delegate review and release authority to the professionals whose job it is currently to handle the mountains of classified materials in the nation's archives -- the archivists themselves.
4. To avoid the occasional problem of sensitive information that has been incorrectly filed or shipped to the archives (e.g., names of agents who truly need protection), set a one-year window at the drop-dead point to allow for a final review of certain narrow categories.
5. More generally, it is vital to build into your proposals standards that will ensure that agency officials who continue to classify and review documents for declassification understand the need to balance legitimate concerns for protecting sensitive information against the public's fundamental right to know.



The National Security Archive

Documenting U.S. Foreign Policy

A Project of the Fund for Peace

DURATION OF CLASSIFICATION POSITION PAPER

RECOMMENDED SOLUTIONS:

Criteria for determining the duration of classification should allow for maximum release while protecting information, release of which could cause identifiable harm.

1. Rules for Cold War-era and other historical records: declassify all documents on U.S. foreign policy and national defense that are at least 10 years old unless release would reveal information on advanced weapons plans and designs, advanced intelligence technologies, intelligence assets, cryptological techniques, or would jeopardize negotiations in progress.
2. Rules for recent and post-Cold War: all documents less than 10 years old including those produced after implementation of the Executive Order will be declassified after 20 years. Exceptions: foreign government documents, advanced weapons plans and designs, advanced intelligence technologies, intelligence assets, and cryptological technologies and techniques.
3. Flexibility: include a public interest balancing test for the declassification of information on intelligence sources and methods. For example, material on communications intercepts should be declassified 20-30 years after use of a code ends or after significant changes in technological capabilities occur.
4. Nuclear weapons design and other technical information that are demonstrably likely to contribute to nuclear proliferation should remain classified. Otherwise, the Restricted Data category should not be used to prevent release of information on such subjects as numbers of weapons and war plans.
5. Transition period of one to two years to allow agencies to review documents that are over ten years old and to flag excluded material before retiring files to the National Archives or Federal Records Center.

EXAMPLES OF TIMELY DECLASSIFICATION OF INFORMATION ON SIGNIFICANT EVENTS.

- Releases of information on U.S. policy toward Iraq during the 1980s
- Publication of Yalta and Potsdam papers 10-15 years after the events
- 1946 Pearl Harbor hearings

MEMO

To: John Podesta
From: Gideon Stein
Date: August 6, 1993
Re: PRESIDENTIAL REVIEW DIRECTIVE ON CLASSIFICATION

Discussion Paper, May 14, 1993 [Revised May 21, 1993]

This Discussion Paper was compiled by Sheryl L. Walter and Steve Aftergood to address various issues raised by the Information Security Oversight Office (ISOO). The following are specific differences between the National Security Archive's proposal and the plan put forth by ISOO. The NSA plan outlined the need for balancing potentially damaging information with the public's right to know. According to the NSA, nothing should be classified merely due to its "type." The NSA plan created a list of categories of information "eligible" for classification:

1. Details of advanced weapons system design and operation.
2. Details of pending military operations.
3. Details of ongoing diplomatic negotiations.
4. Identities of confidential intelligence sources, current cryptographic methods in intelligence, and operations characteristics of advanced intelligence technologies.
5. Change references in the current executive order from "national security" to "national defense."
6. Change references in the current executive order from "foreign relations" to "foreign policy."
7. Change references in the current executive order from "foreign government information" to foreign government documents."
8. Return to the practice of automatic declassification with sunset dates. Compliance should be ensured with a suitable enforcement mechanism.
9. Establish a "universal on-site declassification authority" that would allow for declassification to be conducted by a single review at a single agency; rather than having to rely on multi-agency consultations.
10. Older documents should be declassified in bulk rather than relying on the slow and costly process of page-by-page review.
11. Except for a very limited number of exceptions, all documents older than 20 years should be declassified; also, all archival indices, catalogues, and finding

- guides to government documents should be declassified immediately.
12. All weapons acquisition programs (a chronically problematic category) should not be included in the "special access" list.
 13. Since both the "need to know" provision and classification of documents are too widely used, there should be a reduction in the amount of classified information. This would cause the "need to know" principle to be taken more seriously.
 14. Those who abuse the system and regularly "overclassify" documents should have their classification authority revoked.

ISOO HEARINGS: Changes to the Security Classification Systems
Testimony of Sheryl L. Walter, General Counsel, June 9, 1993
The following is a list of proposed changes to the existing executive order.

1. Establish as the primary standard for classification standards a requirement that there be identifiable damage from release of the information.
2. Balance identifiable harm findings against the public's interest in disclosure.
3. Incorporate real cost-benefit calculations of secrecy into classification decisions.
4. Categories for classified information.
 - a. National defense and pending military operations (not national security)
 - b. Ongoing diplomatic negotiations (not foreign relations)
 - c. Foreign government documents (not foreign government information)
 - d. Identifiable damage to a source.
 - e. Weapons technology and specifications (not the fact or cost of programs)

Testimony of Lynda Davis, FOIA Coordinator and Sheryl L. Walter,
General Counsel, June 9, 1993

1. Prohibit reclassification of information.
2. Weigh the costs and benefits of classifying information by balancing the public interest benefit from release with identifiable harm to the nation.
3. Establish a sunset date of no more than 10 years for every classified document.
4. Reduce the number of departments and original classifiers of information.
5. Set specific timetables for automatic declassification of documents.
6. Identify by name the original classifiers of all documents.
7. Give declassification of information the same or greater emphasis accorded to classification.

8. Provide incentives for challenging improper classification decisions.
9. Create narrow and specific categories of information eligible for classification. [see the five categories listed in Ms. Walter's testimony, no. 4]

Recommendations to the Committee on Oversight of the PRD 29 Task Force, Thomas Blanton, Executive Director of the National Security Archive, June 9, 1993

The following is a list of recommendations for oversight of special access programs.

1. Impose a two year sunset on SAPs classification.
2. Remove weapons acquisition from SAP documents.
3. Establish a long-term goal of abolishing SAPs classifications.
4. Create incentives for employees to challenge the need for SAPs.

Recommendations for Individual Accountability:

5. Put the name of classifier and justification for classification on each document.
6. Impose a sunset on every secret.
7. Provide incentives for employees to challenge classifications.
8. Performance plans and reviews should openness and declassification as criteria for success and promotion.

Oversight:

9. Agencies and ISOO should report annually to relevant Congressional Committees on all SAPs showing progress on the long-term goal of eliminating SAPs.
10. Delegate to ISOO analysts ability to oversee SAPs.
11. Hold hearings and pass a statutory mandate providing for Congressional oversight of the classification system.
12. Each agency needs to identify, by time period, its most sensitive materials; all other materials should be automatically declassified.
13. Create an independent review board for Cold War documents that would establish the criteria for bulk declassification and oversee its implementation.
14. Establish cost-measurement methods for keeping secrets for use in cost-benefit analyses on individual classification decisions.

Recommendations for ISOO Panel on Declassification
Malcolm Byrne, June 10, 1993

1. Mandate bulk declassification after twenty years except for a few special exceptions.
2. Establish an outside independent review board to formulate limited criteria for withholding information.
3. Once guidelines have been set, delegate review and release authority to the archivists.
4. To avoid releasing still sensitive information by mistake, set a one year window at the end of the sunset

period to allow for a final review of certain narrow categories.

5. Establish standards that will ensure that agency officials working on declassification balance legitimate concerns for protecting sensitive information against the public's basic right to know.

To:

John Podesta

from

Steve Kazenfel

PRD 29
TASK FORCE

PHOTOCOPY
PRESERVATION



Information Security Oversight Office
750 17th Street, NW., Suite 530
Washington, DC 20006

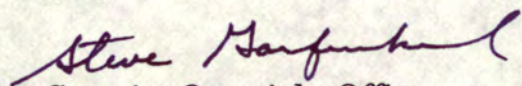


August 4, 1993

MEMORANDUM FOR: The Honorable
John Podesta
Assistant to the President and Staff Secretary

The Honorable
George Tenet
Special Assistant to the President and
Senior Adviser for Intelligence Programs

Michael Waguespack
Director for Counterintelligence Programs
National Security Council

FROM: Steven Garfinkel 
Director, Information Security Oversight Office

SUBJECT: Presidential Review Directive 29

As requested, please find enclosed the following tables:

- Table I: A side-by-side comparison of the major changes to E.O. 12356 as reflected in the draft of July 30; and
- Table II: A list of the changes to E.O. 12356 recommended by the various committees of the interagency task force that ISOO chose not to include in the draft of July 30, and our reasons for not including them.

Please call me if you have any questions or require additional materials for your review.

Enclosures



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.

TABLE I

Divider Title: _____

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Tone</i>	Emphasizes in the Preamble and throughout the Order the need to protect national security information.	Stresses in the Preamble and throughout the Order the Administration's commitment to openness principles and balancing the need to protect critically sensitive information with the public's need to know.	Tone is in keeping with the Administration's commitment to openness and with changes in world conditions.
<i>Definition of Terms</i>	Provides definitions for only some of the terms used throughout the Order. Defines them at the end of the Order.	Refines definitions provided in E.O. 12356. It also provides definitions for terms used throughout the Order, but were not defined in E.O. 12356. Places these definitions at the beginning of each relevant section, instead of listing them at the end of the Order.	Enhances understanding of the provisions of the Order. Increases uniformity in the application of the requirements of the Order by providing clear and unambiguous terms.
<i>Key Term</i>	Uses the term "national security information."	Introduces a new term: "National security protected information."	Makes clear that not all information related to national defense or foreign relations warrants classification.
<i>Classification Standards</i>	No comparable provision. Those standards that appear in the Order are scattered throughout.	Introduces one section listing all the classification standards clearly and concisely.	Promotes more thoughtful original classification decisions by delineating clearly the conditions that must be met to classify originally. Makes it difficult for original classifiers to ignore the standards when they are clearly spelled out.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Accountability for Original Classification</i>	No comparable provision.	Requires classifiers to be able to identify or describe the damage to the national security.	Makes rote classification more difficult by requiring the classifier to be able to identify or describe the damage that would result from unauthorized disclosure. Limits excessive classification. Holds classifiers accountable for their classification decisions.
<i>Balancing Provision</i>	No comparable provision.	Emphasizes the opportunity for original classifiers to weigh the public interest in keeping information unclassified that otherwise meets the standards for classification.	Provides a balancing mechanism so that the public interest in both openness and protection may be considered.
<i>Reasonable Doubt</i>	Permits classification when there is a doubt about the need to classify.	Prohibits classification when there is a doubt about the need to classify.	Reinforces the openness theme set in the Preamble. Sends a clear message to classifiers on the need to use classification with restraint. Leads to fewer questionable classifications.
<i>Classification Levels</i>	Provides for three levels of classification: Top Secret - exceptionally grave damage Secret - serious damage Confidential - damage.	Reduces the levels of classification to two: Top Secret - exceptionally grave damage that the original classifier is able to identify or describe; Secret - damage that the original classifier is able to identify or describe.	Curbs excessive classification by requiring classifiers to be able to identify or describe the damage to the national security. Recognizes that the current Secret and Confidential levels are largely interchangeable.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Classification Levels</i>	Permits classifiers to classify at the higher level when in doubt about the appropriate level.	Requires original classifiers to classify at the lower level when in doubt about the appropriate level.	Curbs the use of the higher classification level. Reduces costs in safeguarding classified information since information classified at a higher level is more expensive to protect.
<i>Classification Categories</i>	Establishes ten categories, each very broad in scope.	Reduces the categories to five, each with a more limited range of application.	Curbs excessive classification by reducing the number of classification categories and narrowing their range.
<i>Training of Original Classifiers</i>	No comparable provision.	Specifies that an original classifier may not exercise such authority until the individual is trained and certified in the Order and its implementing directives.	Promotes greater expertise in classification standards and requirements and accountability for classification decisions. Enhances the quality of classification decisions.
<i>Presumption of Classification</i>	Establishes a presumption of damage for the unauthorized disclosure of certain categories of information.	Eliminates the presumption that any category of information is automatically classified.	Eliminates the automatic classification of information that may not meet classification standards. Encourages U.S. officials handling foreign government information to obtain explicit instructions concerning the sensitivity of the information.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART I OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Portion Marking</i>	Permits agency heads to waive portion marking requirements.	Eliminates waivers of portion marking.	Reduces unnecessary classification that results from the derivative classification of documents that are not portion marked. Facilitates public access to information by making declassification reviews easier since information will be completely portion marked.
<i>Markings</i>	Requires the identity of the original classification authority by name or position if other than the person who signed the pertinent document.	Requires that the name or personal identifier and position of the original classifier be included as one of the essential classification markings.	Fixes responsibility and accountability for original classification actions more precisely. Provides a direct audit trail for challenges or consultation.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Scope of Foreign Government Information</i>	Defines the scope of foreign government information as information received in confidence both expressly and impliedly.	Limits the scope of "foreign government information" to information expressly received in confidence.	Eliminates the presumption that all information obtained on foreign soil or indirectly tied to a foreign official is foreign government information that is to be maintained in confidence, i.e., classified.
<i>Duration of Classification</i>	Encourages classifiers to establish a date or event for declassification at the time of origination. Otherwise, assigns an indefinite duration of classification.	Abolishes the indefinite duration of classification. Unless a specific date or event is provided, establishes a 10 year limit for Secret information and a 15 year limit for Top Secret information. Allows no exceptions at the time of classification, but permits extensions by original classifiers applying classification standards when the information approaches the date of automatic declassification.	Eliminates overclassification associated with the indiscriminate use of the indefinite duration of classification. Requires classifiers to give serious thought about relating the sensitivity of information to a certain date or event. Shortens the life span of classified information, thus reducing costs associated with the administration of the program.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART I OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Reason for Classification</i>	No comparable provision.	Requires that a concise reason for classification be included as one of the essential markings.	Eliminates the question of "why is this classified?" Promotes reasoned classification decisions by requiring classifiers to think about what they are doing.
<i>Use of Classified Addenda</i>	No comparable provision.	Instructs original classifiers to consider the use of a classified addendum when national security protected information constitutes a small portion of an otherwise unclassified document.	Makes more Government information readily available to the public. Reduces the volume of classified documents. Simplifies and expedites classified document review in response to FOIA requests.
<i>Reclassification Prohibition</i>	Allows the reclassification of information previously declassified and disclosed under certain limited conditions.	Prohibits the reclassification of information after it has been declassified and released to the public under proper authority.	Provides an additional incentive for classifiers and declassifiers to make judicious decisions. Removes a provision of E.O. 12356 that many feel is subject to abuse.
<i>Classification by Compilation</i>	By implication, allows for classification by compilation with few if any restrictions.	Restricts the use of classification by compilation and delineates clearly the conditions that must be met for such classification.	Standardizes the treatment of compilations of unclassified information throughout the Government. Prevents excessive classification that results when a compilation of unclassified information is unnecessarily classified.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Challenges to Classification</i>	Encourages challenges to perceived improper classification, but does not provide any mechanism for processing such challenges or protection against retribution.	Requires individuals to challenge classification decisions that they believe to be improper. Directs agencies to establish procedures for processing challenges to classification and ensuring that challengers are not subject to retribution.	Fosters reasoned classification challenges by providing a mechanism for making such challenges. Minimizes the apprehension of challenging classification by assuring that challengers shall not be subject to adverse action. Serves as a deterrent to improper classification decisions.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 2 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Derivative Classifiers</i>	No comparable provisions.	Requires that derivative classification authorities be designated in writing and be trained and certified. Requires that the name or personal identifier of the derivative classifier be included as one of the essential classification markings.	Reduces excessive classification through the designation of more qualified authorized classifiers. Broadens the perspective of derivative classifiers about the classification system. Holds derivative classifiers accountable for their classification decisions.
<i>Classification Guides</i>	Requires agencies with original classification authorities to prepare classification guides, but does not establish a standard for the preparation of a guide. Allows for agency heads to waive this requirement.	Requires that classification guides conform to standards contained in directives issued by the Information Security Oversight Office. Eliminates waivers of the requirement to produce classification guides.	Promotes consistent and accurate classification decisions. Enforces the requirement to produce classification guides. Promotes a better understanding of the basis for classification determinations. Cuts back on the number of original decisions.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 3 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Declassification Balancing Authority</i>	No comparable provision.	Emphasizes the opportunity for a declassification authority to weigh the public interest by declassifying information that otherwise continues to meet the standards for classification.	Allows agency heads or senior agency officials to balance the continued classification of information with the public interest in declassifying the information, permitting declassification even though the information continues to meet the standards for classification.
<i>Declassification of Transferred Information</i>	No comparable provision.	Requires agencies to declassify records of permanent historical value before they may be accessioned into the National Archives.	Prevents the continuing growth of a huge quantity of unprocessed classified records at the National Archives by requiring agencies to declassify records of permanent historical value before they are accessioned into the National Archives.
<i>Automatic Declassification</i>	No comparable provision.	Requires the automatic declassification of information that is 45 years old. Allows agency heads to exempt four very narrow categories of information, for example, the identity of a living human intelligence source. An agency may set a later declassification date for such information..	Establishes a maximum life span for all national security protected information.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 3 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Automatic Declassification</i>	No comparable provision.	Requires that any exempted information remain subject to mandatory and systematic declassification review provisions.	Prevents the indefinite classification of information exempted from the 45-year automatic declassification requirement.
<i>Renegotiation of Treaties or International Agreements</i>	No comparable provision.	Requires the Secretary of State to renegotiate any treaties or international agreements that extend classification beyond 45 years.	Seeks to remedy the unending classification of certain foreign government information that no longer requires protection in the interest of national security.
<i>Systematic Review</i>	Requires the National Archives to review classified permanently valuable (archival) records and presidential papers as they become 30 years old, except for certain intelligence or cryptologic file series, which are reviewed as they become 50 years old.	Requires all originating agencies to establish a systematic declassification review program for records that are 25 years old and to prioritize the program based upon researcher interest and the likelihood of declassification.	Reduces the time frame for the commencement of a systematic review program and shifts the burden of the program from the National Archives, which does not have sufficient resources, to the originating agencies.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 3 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Declassification Guides</i>	No comparable provision.	Requires the Information Security Oversight Office to assure that the declassification guides developed by the agencies and furnished to the National Archives are adequate and current.	Seeks to improve the systematic review process by assuring that the guidance is adequate to facilitate declassification.
<i>Mandatory Declassification Review</i>	No comparable provision.	Excuses agencies from the requirement to conduct a mandatory declassification review when the same information has been reviewed within the prior two years.	Remedies overlapping declassification reviews of the same or similar information, allowing agencies to devote resources to reviews more likely to result in declassification.
<i>Declassification Database</i>	No comparable provision.	Requires the Archivist, in conjunction with the agencies and the Information Security Oversight Office, to explore the feasibility of a Government-wide declassification database and requires the Archivist to explore further uses of technology to assist the declassification process.	Seeks a Government-wide declassification database that will greatly enhance the process through the avoidance of duplication and non-uniform results.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 4 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Restriction on Removal of Classified Information</i>	No comparable provision.	Prevents departing Government officials from removing classified information from the agency's control.	Prevents the situation of Government officials leaving Government service and taking classified materials with them. States explicitly what has only been implied before.
<i>AIS Safeguards</i>	No comparable provision.	Emphasizes the requirement to safeguard classified information in automated information systems.	Clarifies position that safeguards for classified information must include the protection of automated information systems that process such information.
<i>"Third Agency Rule"</i>	Requires that classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency.	Permits an originating agency to waive the requirement that another agency receive permission before it can disclose the first agency's information to a third agency.	Improves interagency dissemination of classified information by allowing the "third agency rule" to be waived by the originating agency in appropriate cases.
<i>Distribution Control</i>	No comparable provision.	Requires the annual update of any automatic, routine or recurring distribution list of classified information.	Establishes controls over the automatic distribution of classified information, which: saves costs in reproduction and distribution; enforces need-to-know; helps reduce overdistribution of classified information; and helps to reduce the number of unauthorized disclosures.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 4 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Establishment of Special Access Programs</i>	Requires heads of agencies to provide written authorization for the creation or continuation of a special access program.	Limits, generally, the establishment of special access programs to the Secretaries of State, Defense and Energy, and the Director of Central Intelligence or their principle deputies.	Seeks to reduce significantly the number of special access programs by limiting their creation to the highest level officials of a few agencies.
<i>Establishment of Special Access Programs</i>	No comparable provision.	Defines and limits what kind of circumstances must exist before an agency head may establish a special access program.	Seeks to reduce significantly the number of special access programs by establishing standards and definitions that limit their authorization.
<i>Oversight of Special Access Programs</i>	Requires heads of agencies to establish and maintain a system of accounting for special access programs and provide the Director of the ISOO nondelegable access to all such accounts.	Requires internal oversight and oversight by the Information Security Oversight Office for all special access programs.	Increases significantly the internal and external oversight of special access programs.
<i>Oversight of Special Access Programs</i>	No comparable provision.	Requires that any special access program be revalidated annually.	Provides another control on the number and increases oversight of special access programs by requiring annual revalidation at the agency head or deputy level.
<i>Duration of Special Access Programs</i>	No comparable provision.	Requires unanimous approval of an executive committee of agency heads in order to continue any special access program beyond five years.	Limits special access programs that go beyond five years to those that will be endorsed by a unanimous committee of agency heads.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 4 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Revalidation of Existing Special Access Programs</i>	No comparable provision.	Requires the agency head or principal deputy to review for revalidation any special access program that predates this Order.	Provides an immediate mechanism to assess special access programs created under prior orders.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 5 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Authority of ISOO</i>	Requires ISOO Director to appeal agency denials of access to the National Security Council.	Requires agency to justify in writing to the National Security Council when it seeks to deny access to ISOO.	Places the onus on agency heads rather than ISOO in situations where agencies seek to deny access to ISOO. Increases ISOO's oversight capability.
<i>ISOO Directives</i>	No comparable provision.	Requires ISOO Director to issue directives that establish uniform standards for safeguarding; security education and training; agency self-inspections; and classification and declassification guides.	Establishes a system designed to result in cost savings through uniformity and the application of reasonable risk management principles.
<i>Policy Advisory Council</i>	No comparable provision.	Establishes an Information Security Policy Advisory Council consisting of Government and Non-Government representatives.	Provides a forum for interested organizations outside the Government to express their concerns about the system and to interact with those responsible for the system within Government.
<i>Accountability of Top Management</i>	No comparable provision.	Requires heads of agencies to demonstrate personal and senior management commitment for the effective implementation of the program.	Remedies a major shortfall in the current system by emphasizing the role and responsibility of senior management for the success of the program, rather than simply delegating the onus to non-policy security officials.

COMPARISON OF MAJOR FEATURES OF E.O. 12356 AND DRAFT ORDER DATED JULY 30, 1993

PART 5 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED JULY 30	IMPROVEMENT
<i>Individual Accountability</i>	No comparable provision.	Requires that the performance contracts of critical personnel, including classifiers and security professionals, include the management of classified information as an element of performance to be evaluated annually.	Increases individual accountability for the effectiveness of the system by tying its management to the performance contracts or plans of its most important implementers, including original classifiers.
<i>Accounting for Costs</i>	No comparable provision.	Requires agencies to account for all costs associated with the security classification program and to submit those costs annually to ISOO for publication.	Enables the executive branch to account for the costs of the classification system, rather than simply speculate, as a means of cost control.
<i>Sanctions</i>	No comparable provision.	Requires sanctions when an individual creates or continues a special access program contrary to the requirements of the Order.	Establishes a further control mechanism to prevent the creation or continuance of unnecessary special access programs.
<i>Sanctions</i>	No comparable provision.	Requires the prompt removal of classification authority from an individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of the Order.	Seeks to remedy the current situation in which, despite the general reference to sanctions for improper classification, such sanctions never seem to be imposed. Requires the prompt removal of classification authority while other sanctions are considered.

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.

TABLE II

Divider Title: _____

COMMITTEE RECOMMENDATIONS NOT ACCEPTED

COMMITTEE	RECOMMENDATION	REASON(S) FOR NONACCEPTANCE
<i>Classification Standards</i>	Create a single level classification system, which includes normal and special protection requirements.	1. Reducing a three level system to a one level system will be far more difficult to implement than reducing to a two level system, especially in the area of personnel security. 2. ISOO is concerned that creating a one level classification system would dominate the review process and detract from other more important changes. 3. ISOO's discussions with the Joint Security Commission revealed that it will recommend a two level classification system.
<i>Excessive Classification</i>	Delete section 1.6(d) of E.O. 12356, which allows reclassification after receipt of a request under FOIA, Privacy Act of 1974 or Mandatory Review provisions of the Order.	1. As long as information has not been publicly disclosed, agencies should not be prevented from classifying information that clearly meets the standards for classification under the July 30, 1993 draft order. This is especially true under this draft, since many classifications will lapse automatically without the opportunity for review. 2. The July 30, 1993 draft order places more stringent requirements on classifying information that has been requested under the FOIA, Privacy Act of 1974 or Mandatory Review provisions.

COMMITTEE	RECOMMENDATION	REASON(S) FOR NONACCEPTANCE
<i>Duration</i>	Allow originating agencies with subject matter authority to set duration standards; automatic declassification would occur in three years if standards are not set.	1. Leaves a critical issue unresolved. 2. Promotes non-uniformity in the application of classification duration. 3. Could result in information being classified longer than necessary.
<i>Declassification</i>	Authorize second agency holders to declassify an originating agency's records through the use of declassification guides.	1. By instituting other reforms, such as requiring agencies to conduct systematic declassification review, before having records accessioned into the National Archives, this provision becomes unnecessary. 2. Agencies are extremely reluctant to delegate declassification authority to another agency.
<i>Declassification</i>	Establish an automatic declassification date at 50 years for all permanently valuable records with no exceptions.	1. The 50 year time frame sounded too long. 2. ISOO's experience indicates that very narrow exceptions are necessary, e.g., the identity of a living human intelligence source.
<i>Oversight</i>	Attach ISOO to the National Security Council.	Decisions concerning placement of ISOO have been put on hold pending the outcome of the appropriations process.

COMMITTEE	RECOMMENDATION	REASON(S) FOR NONACCEPTANCE
<i>Access and Dissemination</i>	Assign agency Inspector General oversight responsibilities of safeguarding controls for classified information.	1. Internal oversight requires on-going review, not just scheduled audits. 2. An agency's internal oversight role is broader than the narrow focus of an Inspector General's audit. 3. Current program will permit role for Inspector General at the Inspector General's option.
<i>Access and Dissemination</i>	Require historical researchers and former Presidential appointees to meet a trustworthiness requirement and sign a non-disclosure agreements.	Inaccurately suggests instituting a more restrictive standard than currently exists in the implementing directive for E. O. 12356.
<i>Safeguarding</i>	Require ISOO to establish and oversee a national information systems security infrastructure and implement it through the National Security Telecommunications and Information Systems Security Committee.	1. Possibly violates current statutes on information systems security. 2. Conflicts with current infrastructure established for information systems security. 3. ISOO does not have the personnel or resources to perform these functions.



Information Security Oversight Office
750 17th Street, NW., Suite 530
Washington, DC 20006



August 16, 1993

MEMORANDUM FOR: The Honorable John Podesta
Assistant to the President and Staff Secretary

The Honorable George Tenet
Special Assistant to the President and
Senior Adviser for Intelligence Programs

Michael Waguespack
Director for Counterintelligence Programs
National Security Council

Neal Wolin
Deputy Legal Adviser, National Security Council

FROM: Steven Garfinkel 
Director, Information Security Oversight Office

SUBJECT: Presidential Review Directive 29: August 17 Draft

Following up on our most recent meeting and telephone conversations, please find enclosed the following materials for your review and comment:

- Tab 1: Highlights of the major changes in the August 17 draft from E.O. 12356.
- Tab 2: A listing of all the major changes, presented in the order that they appear in the August 17 draft.
- Tab 3: A side-by-side comparison between E.O. 12356 and the August 17 draft.
- Tab 4: A chart showing how declassification works under the August 17 draft.
- Tab 5: A clean copy of the August 17 draft.
- Tab 6: A copy of the August 17 draft in legislative drafting style, showing the changes from the current Order.



In Tab 5, we have placed in bold face each paragraph that has been revised or is new from the July 30 draft, even if the change is only a word or two. Also, we attach to this cover memo six possible formulations of the make-up of the Interagency Security Classification Appeals Panel, which is established in the revised Section 5.4 of the draft. Obviously, mixing, matching and substituting would permit a number of additional formulations. We prefer the first formulation, which appears in the full draft, because: (a) it will be the most practical; (b) it doesn't undermine ISOO's oversight role; and (c) **none** of the formulations that should be given serious consideration will satisfy some critics' demands that an independent appeal body consist of outsiders.

Finally, with respect to the Appeals Panel, in the draft we have included the option mentioned at our meeting of the Panel taking appeals from agency Freedom of Information denials for classified information. We recommend that its functions not include Freedom of Information Act appeals. Including these will increase its workload tremendously, without any additional good will benefits. Persons who wish to take advantage of the Panel rather than having to resort to litigation can simply file mandatory review requests rather than Freedom of Information requests.

As I mentioned at our meeting, I will be home entertaining out-of-towners from Tuesday afternoon, August 17, through the rest of the week. Because of our desire to get this to the agencies as early as possible, I look forward to discussing your decisions and revisions by telephone. I can be reached at home at (301) 384-4513. If I do not hear from you by Wednesday afternoon, I'll call Neal on Thursday morning.

Enclosures and Attachments

SIX ALTERNATIVES FOR SECTION 5.4(a)

ALTERNATIVE 1. (a) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Director of the Information Security Oversight Office shall serve as Chairman of the Panel. The Secretaries of State and Defense, the Attorney General and the Director of Central Intelligence shall each appoint a senior level employee to comprise the other members of the Panel.

ALTERNATIVE 2. (a) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Associate Attorney General shall serve as Chairman of the Panel. The other members of the Panel shall include the Director of the Information Security Oversight Office and a senior level employee appointed respectively by the Secretaries of State and Defense, and the Director of Central Intelligence.

ALTERNATIVE 3. (a) There is established an Interagency Security Classification Appeals Panel ("Panel"). The President shall appoint its members from among persons nominated by the Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, and the Director of the Information Security Oversight Office. The members of the Panel shall elect the Chairman.

ALTERNATIVE 4. (a) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Associate Attorney General shall serve as Chairman of the Panel. The other members of the Panel shall include the Director of the Information Security Oversight Office and the senior legal officer of the Departments of State and Defense, and the Central Intelligence Agency.

ALTERNATIVE 5. (a) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Deputy Attorney General shall serve as Chairman of the Panel. The other members of the Panel shall include the principal deputy of the Departments of State, Defense and Energy, and the Central Intelligence Agency.

ALTERNATIVE 6. (a) There is established an Interagency Security Classification Appeals Panel ("Panel"). The five members of the Panel, including its Chairman, shall be appointed by the President.

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: _____

HIGHLIGHTS OF MAJOR CHANGES

- Sets a positive tone by stressing the Administration's commitment to the democratic principle of open government.
- Emphasizes the opportunity for original classifiers to weigh the public interest in keeping information unclassified that otherwise meets the standards for classification.
- Emphasizes the opportunity for a declassification authority to weigh the public interest by declassifying information that otherwise continues to meet the standards for classification.
- Requires heads of agencies to demonstrate personal and senior management commitment for the effective implementation of this program.
- Abolishes the indefinite duration of classification, or "Originating Agency's Determination Required" (OADR).
- Establishes a maximum life span for all national security protected information.
- Curbs excessive classification by reducing the number of classification categories from 10 to 5, and narrowing their range of application.
- Prohibits classification when there is a reasonable doubt about the need to classify.
- Eliminates the presumption that any category of information is automatically classified.
- Requires the prompt removal of classification authority from an individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of the Order.
- Prohibits the reclassification of information after it has been declassified and released to the public under proper authority.
- Reduces the levels of classification to two, **Top Secret** and **Secret**.

- Curbs excessive classification by requiring original classifiers to be able to identify or describe the damage to the national security that could result from the unauthorized disclosure of the information.
- Limits special access programs to meet narrow and specific criteria.
- Establishes an Interagency Security Classification Appeals Panel of senior government officials to serve as the last appellate authority for classification challenges, or mandatory review or Freedom of Information Act appeals for access to national security protected information.
- Establishes an Information Security Policy Advisory Council consisting of Government and non-Government representatives to advise on matters concerning policies established under the Order, including recommended changes to those policies.
- Requires agencies to account for all costs associated with the security classification program and to report those costs to the Information Security Oversight Office for publication.
- Eliminates portion marking waivers.
- Requires that derivative classification authorities be designated in writing and be trained and certified.
- Eliminates waivers of the requirement to produce classification guides.
- Requires all originating agencies to establish a systematic declassification review program for all records that are 25 years old.

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: _____

**MAJOR CHANGES
CONTAINED IN AUGUST 17, 1993
DRAFT EXECUTIVE ORDER ON
NATIONAL SECURITY PROTECTED INFORMATION
(IN ORDER OF APPEARANCE IN THE DRAFT)**

- Sets a positive tone by stressing the Administration's commitment to the democratic principle of open government. [Preamble]
- Acknowledges the need to balance the protection of critically sensitive information in the interest of the national security with that of promoting the flow of information essential for the nation's progress. [Preamble]
- Underscores the fact that dramatic geopolitical changes have altered the nature of security threats and that corresponding changes in classification policies are required. [Preamble]
- Promotes understanding of the Order by providing clear definitions of key terms at the beginning of each major section. [1.1; 2.1; 3.1; 4.1; and 5.1]
- Introduces a new term, "national security protected information," narrower in scope than the current "national security information." [1.1(c)]
- Promotes more reasoned classification decisions by grouping under one section the standards for original classification that are scattered throughout the current Order. [1.2(a)]
- Delineates clearly the conditions that original classifiers must meet in order to classify information in the first instance. [1.2(a)]
- Curbs excessive classification by requiring original classifiers to be able to identify or describe the damage to the national security that could result from the unauthorized disclosure of the information. [1.2(a)(4)]
- Emphasizes the opportunity for original classifiers to weigh the public interest in keeping information unclassified that otherwise meets the standards for classification. [1.2(b)]
- Prohibits classification when there is a reasonable doubt about the need to classify. [1.2(c)]
- Reduces the levels of classification to two, **Top Secret** and **Secret**. [1.3(a)]

- Requires original classifiers to classify information at the lower level when in doubt about the appropriate level of classification. [1.3(c)]
- Directs that information classified **Confidential** under predecessor orders be declassified no later than six years from the effective date of this Order. Continued classification requires a new original classification decision to upgrade such information to **Secret**. [1.3(d)]
- Limits the authority to designate original classification authority. [1.4(c)]
- Specifies that an original classification authority may not exercise such authority until the individual is trained and certified as provided in the Order and its implementing directives. [1.4(d)]
- Curbs excessive classification by reducing the number of classification categories from 10 to 5, and narrowing their range of application. [1.5]
- Eliminates the presumption that any category of information is automatically classified.
- Abolishes the indefinite duration of classification, or "Originating Agency's Determination Required" (OADR).
- Eliminates portion marking waivers.
- Establishes a timetable for automatic declassification when original classifiers cannot determine a date or event for declassification. [1.6 (b), (c) and (d)]
- Encourages automatic declassification by restricting extensions of the duration of classification. [1.6(e)]
- Requires that the name or personal identifier of the original classification authority be included as one of the essential classification markings. [1.7(a)(2)]
- Requires that a concise reason for classification be included as one of the essential classification markings. [1.7(a)(5)]
- Instructs original classifiers to use, whenever practicable, a classified addendum when national security protected information constitutes a small portion of an otherwise unclassified document. [1.7(g)]
- Prohibits the reclassification of information after it has been declassified and released to the public under proper authority. [1.8(c)]

- Restricts the use of classification by compilation and delineates clearly the conditions that must be met for such classifications. [1.8(e)]
- Requires individuals to challenge classification decisions that they believe to be improper. [1.9(a)]
- Directs agencies to establish procedures for processing challenges to classification and ensuring that challengers are not subject to retribution. [1.9(b)]
- Requires that derivative classification authorities be designated in writing and be trained and certified. [2.2(a)]
- Requires that the name or personal identifier of the derivative classifier be included as one of the essential classification markings. [2.2(c)(2)(A)]
- Requires that classification guides conform to standards contained in directives issued by the Information Security Oversight Office. [2.3(a)]
- Requires periodic review and update of classification guides. [2.3(c)]
- Eliminates waivers of the requirement to produce classification guides. [2.3]
- Emphasizes the opportunity for a declassification authority to weigh the public interest by declassifying information that otherwise continues to meet the standards for classification. [3.2(b)]
- Requires agencies to declassify records of permanent historical value before they may be accessioned into the National Archives. [3.3(d)]
- Establishes a maximum life span for all national security protected information. [3.4(a)]
- Permits, after justification and approval, the exemption of four very narrow categories of information from the 40-year automatic declassification requirement. [3.4(b)]
- Requires that any exempted information remain subject to mandatory and systematic declassification review provisions. [3.4(d)]
- Requires the Secretary of State to renegotiate any treaties or international agreements that extend classification beyond 40 years. [3.4(e)]

- Requires all originating agencies to establish a systematic declassification review program for all records that are 25 years old. [3.5(a)]
- Requires agencies to prioritize the systematic declassification review program based upon researcher interest and likelihood of declassification. [3.5(a)]
- Requires the Information Security Oversight Office to assure that the declassification guides developed by the agencies and furnished to the National Archives are adequate and current. [3.5(b)]
- Excuses agencies from the requirement to conduct a mandatory declassification review when the same information has been reviewed within the prior two years. [3.6(a)(3)]
- Requires the Archivist, in conjunction with the agencies and the Information Security Oversight Office, to establish a Government-wide declassification database. [3.8]
- Requires the Archivist to explore further uses of technology to assist the declassification process. [3.8]
- Prevents departing Government officials from removing national security protected information from the agency's control. [4.2(b)]
- Emphasizes the requirement to safeguard national security protected information in automated information systems. [4.2(e)]
- Permits an originating agency to waive the requirement that another agency receive permission before it can disclose the first agency's information to a third agency. [4.2(g)]
- Requires the annual update of any automatic, routine or recurring distribution lists of national security protected information. [4.3(b)]
- Limits, generally, the establishment of special access programs to the Secretaries of State, Defense and Energy, and the Director of Central Intelligence or their principal deputies. [4.4(a)]
- Limits special access programs to meet narrow and specific criteria. [4.4(a) and (b)]
- Requires internal oversight and oversight by the Information Security Oversight Office for all special access programs. [4.4(b)(3)]

- Requires that any special access program be revalidated annually. [4.4(b)(4)]
- Requires unanimous approval of an executive committee of agency heads in order to continue any special access program beyond five years. [4.4(b)(5)]
- Requires the agency head or principal deputy to review for revalidation any special access program that predates this Order. [4.4(c)]
- Directs an agency to submit a written justification to the National Security Council when seeking to deny access to the Information Security Oversight Office. [5.3(b)(4)]
- Requires the Director of the Information Security Oversight Office, through directives, to establish uniform standards for safeguarding; security education and training programs; agency self-inspection programs; and classification and declassification guides. [5.3(c)]
- Establishes an Interagency Security Classification Appeals Panel of senior Government officials to serve as the last appellate authority for classification challenges and mandatory review appeals. [5.4]
- Establishes an Information Security Policy Advisory Council consisting of Government and non-Government representatives to advise on matters concerning policies established under the Order, including recommended changes to those policies. [5.5]
- Requires heads of agencies to demonstrate personal and senior management commitment for the effective implementation of this program. [5.6(a)(1)]
- Increases individual accountability by tying performance contracts to the effective implementation of this program. [5.6(a)(3)(G)]
- Requires agencies to account for all costs associated with the security classification program and to submit those costs to the Information Security Oversight Office for publication. [5.6(a)(3)(H)]
- Directs Inspectors General to conduct periodic audits of programs established under this Order. [5.6(b)]
- Requires sanctions when an individual creates or continues a special access program contrary to the requirements of the Order. [5.7 (b)(3)]

- Requires the prompt removal of classification authority from an individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of the Order. [5.7(d)]

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: _____

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 1 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Tone</i>	Emphasizes in the Preamble and throughout the Order the need to protect national security information.	Stresses in the Preamble and throughout the Order the Administration's commitment to openness principles and balancing the need to protect critically sensitive information with the public's need to know.	Tone is in keeping with the Administration's commitment to openness and with changes in world conditions.
<i>Definition of Terms</i>	Provides definitions for only some of the terms used throughout the Order. Defines them at the end of the Order.	Refines definitions provided in E.O. 12356. It also provides definitions for terms used throughout the Order, but were not defined in E.O. 12356. Places these definitions at the beginning of each relevant section, instead of listing them at the end of the Order.	Enhances understanding of the provisions of the Order. Increases uniformity in the application of the requirements of the Order by providing clear and unambiguous definitions of terms.
<i>Key Term</i>	Uses the term "national security information."	Introduces a new term: "National security protected information."	Makes clear that not all information related to national defense or foreign relations warrants classification.
<i>Classification Standards</i>	No comparable provision. Those standards that appear in the Order are scattered throughout.	Introduces one section listing all the classification standards clearly and concisely.	Promotes more thoughtful original classification decisions by delineating clearly the conditions that must be met to classify originally. Makes it difficult for original classifiers to ignore the standards when they are clearly spelled out.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Accountability for Original Classification</i>	No comparable provision.	Requires classifiers to be able to identify or describe the damage to the national security.	Makes rote classification more difficult by requiring the classifier to be able to identify or describe the damage that would result from unauthorized disclosure. Limits excessive classification. Holds classifiers accountable for their classification decisions.
<i>Balancing Provision</i>	No comparable provision.	Emphasizes the opportunity for original classifiers to weigh the public interest in keeping information unclassified that otherwise meets the standards for classification.	Provides a balancing mechanism so that the public interest in both openness and protection may be considered.
<i>Reasonable Doubt</i>	Permits classification when there is a doubt about the need to classify.	Prohibits classification when there is a doubt about the need to classify.	Reinforces the openness theme set in the Preamble. Sends a clear message to classifiers on the need to use classification with restraint. Leads to fewer questionable classifications.
<i>Classification Levels</i>	Provides for three levels of classification: Top Secret - exceptionally grave damage Secret - serious damage Confidential - damage	Reduces the levels of classification to two: Top Secret - grave damage that the original classifier is able to identify or describe; Secret - damage that the original classifier is able to identify or describe.	Curbs excessive classification by requiring classifiers to be able to identify or describe the damage to the national security. Recognizes that the current Secret and Confidential levels are largely interchangeable.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 1 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Classification Levels</i>	Permits classifiers to classify at the higher level when in doubt about the appropriate level.	Requires original classifiers to classify at the lower level when in doubt about the appropriate level.	Curbs the use of the higher classification level. Reduces costs in safeguarding classified information since information classified at a higher level is more expensive to protect.
<i>Delegation of Original Classification Authority</i>	Restricts delegations of Top Secret original classification authority to the President, agency heads, officials designated by the President in the <i>Federal Register</i> , and agency senior officials for oversight. Restricts delegations of Secret and Confidential original authority to the President, agency heads, officials designated by the President in the <i>Federal Register</i> , officials with original Top Secret classification authority, and the agency senior official for oversight.	Restricts delegation of original (i) Top Secret classification authority to the President or agency heads and officials designated by the President in the <i>Federal Register</i> ; and (ii) Secret classification authority to the individuals listed above and, the agency senior official for oversight provided that individual has been delegated Top Secret authority.	Reduces the number of officials who may designate original classification authorities. Increases controls over the delegation of original classification authority.
<i>Classification Categories</i>	Establishes ten categories, each very broad in scope.	Reduces the categories to five, each with a more limited range of application.	Curbs excessive classification by reducing the number of classification categories and narrowing their range.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Training of Original Classifiers</i>	No comparable provision.	Specifies that an original classifier may not exercise such authority until the individual is trained and certified in the Order and its implementing directives.	Promotes greater expertise in classification standards and requirements and accountability for classification decisions. Enhances the quality of classification decisions.
<i>Presumption of Classification</i>	Establishes a presumption of damage for the unauthorized disclosure of certain categories of information.	Eliminates the presumption that any category of information is automatically classified.	Eliminates the automatic classification of information that may not meet classification standards. Encourages U.S. officials handling foreign government information to obtain explicit instructions concerning the sensitivity of the information.
<i>Portion Marking</i>	Permits agency heads to waive portion marking requirements.	Eliminates waivers of portion marking.	Reduces unnecessary classification that results from the derivative classification of documents that are not portion marked. Facilitates public access to information by making declassification reviews easier since information will be completely portion marked.
<i>Markings</i>	Requires the identity of the original classification authority by name or position if other than the person who signed the pertinent document.	Requires that the name or personal identifier and position of the original classifier be included as one of the essential classification markings.	Fixes responsibility and accountability for original classification actions more precisely. Provides a direct audit trail for challenges or consultation.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Scope of Foreign Government Information</i>	Defines the scope of "foreign government information" as information received in confidence both expressly and impliedly.	Limits the scope of "foreign government information" to information expressly received in confidence.	Eliminates the presumption that all information obtained on foreign soil or indirectly tied to a foreign official is "foreign government information" that is to be maintained in confidence, i.e., classified.
<i>Duration of Classification</i>	Encourages classifiers to establish a date or event for declassification at the time of origination. Otherwise, assigns an indefinite duration of classification.	Abolishes the indefinite duration of classification. Unless a specific date or event is provided, establishes a 10 year limit for Secret information and a 15 year limit for Top Secret information. Allows no exceptions at the time of classification, but permits extensions by original classifiers applying classification standards when the information approaches the date of automatic declassification.	Eliminates overclassification associated with the indiscriminate use of the indefinite duration of classification. Requires classifiers to give serious thought about relating the sensitivity of information to a certain date or event. Shortens the life span of classified information, thus reducing costs associated with the administration of the program.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Reason for Classification</i>	No comparable provision.	Requires that a concise reason for classification be included as one of the essential markings.	Eliminates the question of "why is this classified?" Promotes reasoned classification decisions by requiring classifiers to think about what they are doing.
<i>Use of Classified Addenda</i>	No comparable provision.	Instructs original classifiers to use, whenever practicable, a classified addendum when national security protected information constitutes a small portion of an otherwise unclassified document.	Makes more Government information readily available to the public. Reduces the volume of classified documents. Simplifies and expedites classified document review in response to FOIA requests.
<i>Reclassification Prohibition</i>	Allows the reclassification of information previously declassified and disclosed under certain limited conditions.	Prohibits the reclassification of information after it has been declassified and released to the public under proper authority.	Provides an additional incentive for classifiers and declassifiers to make judicious decisions. Removes a provision of E.O. 12356 that many feel is subject to abuse.
<i>Classification by Compilation</i>	By implication, allows for classification by compilation with few if any restrictions.	Restricts the use of classification by compilation and delineates clearly the conditions that must be met for such classification.	Standardizes the treatment of compilations of unclassified information throughout the Government. Prevents excessive classification that results when a compilation of unclassified information is unnecessarily classified.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 1 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Challenges to Classification</i>	Encourages challenges to perceived improper classification, but does not provide any mechanism for processing such challenges or protection against retribution.	Requires individuals to challenge classification decisions that they believe to be improper. Directs agencies to (i) establish procedures for processing challenges to classification; (ii) ensure that challengers are not subject to retribution; (iii) provide for review by an impartial official or panel; and (iv) advise the challenger of his or her right to appeal the agency decision.	Fosters reasoned classification challenges by providing a mechanism for making such challenges. Minimizes the apprehension of challenging classification by assuring that challengers shall not be subject to adverse action. Compels agencies to give serious consideration to such challenges by (i) providing for an impartial review, and (ii) allowing the challenger to appeal the agency decision.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 2 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Derivative Classifiers</i>	No comparable provision.	Requires that derivative classification authorities be designated in writing and be trained and certified. Requires that the name or personal identifier of the derivative classifier be included as one of the essential classification markings.	Reduces excessive classification through the designation of more qualified authorized classifiers. Broadens the perspective of derivative classifiers about the classification system. Holds derivative classifiers accountable for their classification decisions.
<i>Classification Guides</i>	Requires agencies with original classification authority to prepare classification guides, but does not establish a standard for the preparation of a guide. Allows for agency heads to waive this requirement.	Requires that classification guides conform to standards contained in directives issued by the Information Security Oversight Office. Eliminates waivers of the requirement to produce classification guides.	Promotes consistent and accurate classification decisions. Enforces the requirement to produce classification guides. Promotes a better understanding of the basis for classification determinations. Cuts back on the number of original decisions.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 3 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Declassification Balancing Authority</i>	No comparable provision.	Emphasizes the opportunity for a declassification authority to weigh the public interest by declassifying information that otherwise continues to meet the standards for classification.	Allows agency heads or senior agency officials to balance the continued classification of information with the public interest in declassifying the information, permitting declassification even though the information continues to meet the standards for classification.
<i>Declassification of Transferred Information</i>	No comparable provision.	Requires agencies to declassify records of permanent historical value before they may be accessioned into the National Archives.	Prevents the continuing growth of a huge quantity of unprocessed classified records at the National Archives by requiring agencies to declassify records of permanent historical value before they are accessioned into the National Archives.
<i>Automatic Declassification</i>	No comparable provision.	Requires the automatic declassification of information that is 40 years old. Allows agency heads to exempt four very narrow categories of information, for example, the identity of a human intelligence source. An agency may set a later declassification date for such information.	Establishes a maximum life span for all national security protected information.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 3 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Automatic Declassification</i>	No comparable provision.	Requires that all national security protected information created more than 40 years before the issuance of this Order, be declassified within two years after its issuance.	Reduces dramatically the amount of older classified material in current holdings. Demonstrates to the public the Administration's commitment to open Government.
<i>Automatic Declassification</i>	No comparable provision.	Requires that any exempted information remain subject to mandatory and systematic declassification review provisions.	Prevents the indefinite classification of information exempted from the 40-year automatic declassification requirement.
<i>Renegotiation of Treaties or International Agreements</i>	No comparable provision.	Requires the Secretary of State to renegotiate any treaties or international agreements that extend classification beyond 40 years.	Seeks to remedy the unending classification of certain foreign government information that no longer requires protection in the interest of national security.
<i>Systematic Review</i>	Requires the National Archives to review classified permanently valuable (archival) records and presidential papers as they become 30 years old, except for certain intelligence or cryptologic file series, which are reviewed as they become 50 years old.	Requires all originating agencies to establish a systematic declassification review program for records that are 25 years old and to prioritize the program based upon researcher interest and the likelihood of declassification.	Reduces the time frame for the commencement of a systematic review program and shifts the burden of the program from the National Archives, which does not have sufficient resources, to the originating agencies.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 3 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
Declassification Guides	No comparable provision.	Requires the Information Security Oversight Office to assure that the declassification guides developed by the agencies and furnished to the National Archives are adequate and current.	Seeks to improve the systematic review process by assuring that the guidance is adequate to facilitate declassification.
Mandatory Declassification Review	No comparable provision.	Excuses agencies from the requirement to conduct a mandatory declassification review when the same information has been reviewed within the prior two years.	Remedies overlapping declassification reviews of the same or similar information, allowing agencies to devote resources to reviews more likely to result in declassification.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 3 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Mandatory Declassification Review</i>	Provides that any decision by the Archivist regarding presidential records may be appealed to the Director of the Information Security Oversight Office.	Establishes an Interagency Security Classification Appeals Panel responsible for deciding appeals of mandatory declassification review denials.	Broadens the deliberative process for appeals of mandatory declassification review denials.
<i>Declassification Database</i>	No comparable provision.	Requires the Archivist, in conjunction with affected agencies and the Information Security Oversight Office, to establish a Government-wide declassification database. Also requires the Archivist to explore further uses of technology to assist the declassification process.	Seeks a Government-wide declassification database that will greatly enhance the process through the avoidance of duplication and non-uniform results.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 4 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Restriction on Removal of Classified Information</i>	No comparable provision.	Prevents departing Government officials from removing classified information from the agency's control.	Prevents the situation of Government officials leaving Government service and taking classified materials with them. States explicitly what has only been implied before.
<i>AIS Safeguards</i>	No comparable provision.	Emphasizes the requirement to safeguard classified information in automated information systems.	Clarifies position that safeguards for classified information must include the protection of automated information systems that process such information.
<i>"Third Agency Rule"</i>	Requires that classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency.	Permits an originating agency to waive the requirement that another agency receive permission before it can disclose the first agency's information to a third agency.	Improves interagency dissemination of classified information by allowing the "third agency rule" to be waived by the originating agency in appropriate cases.
<i>Distribution Controls</i>	No comparable provision.	Requires the annual update of any automatic, routine or recurring distribution list of classified information.	Establishes controls over the automatic distribution of classified information, which: (i) saves costs in reproduction and distribution; (ii) enforces need-to-know; (iii) reduces overdistribution of classified information; and (iv) reduces the number of unauthorized disclosures.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 4 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Establishment of Special Access Programs</i>	No comparable provision.	Defines and limits what kind of circumstances must exist before an agency head may establish a special access program.	Seeks to reduce significantly the number of special access programs by establishing standards and definitions that limit their authorization.
<i>Oversight of Special Access Programs</i>	Requires heads of agencies to establish and maintain a system of accounting for special access programs and provide the Director of the ISOO nondelegable access to all such accounts.	Requires internal oversight and oversight by the Information Security Oversight Office for all special access programs.	Increases significantly the internal and external oversight of special access programs.
<i>Oversight of Special Access Programs</i>	No comparable provision.	Requires that any special access program be revalidated annually.	Provides another control on the number and increases oversight of special access programs by requiring annual revalidation at the agency head or deputy level.
<i>Duration of Special Access Programs</i>	No comparable provision.	Requires unanimous approval of an executive committee of agency heads in order to continue any special access program beyond five years.	Limits special access programs that go beyond five years to those that will be endorsed by a unanimous committee of agency heads.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 4 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Revalidation of Existing Special Access Programs</i>	No comparable provision.	Requires the agency head or principal deputy to review for revalidation any special access program that predates this Order.	Provides an immediate mechanism to assess special access programs created under prior orders.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 5 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Authority of ISOO</i>	Requires ISOO Director to appeal agency denials of access to the National Security Council.	Requires agency to justify in writing to the National Security Council when it seeks to deny access to ISOO.	Places the onus on agency heads rather than ISOO in situations where agencies seek to deny access to ISOO. Increases ISOO's oversight capability.
<i>ISOO Directives</i>	No comparable provision.	Requires ISOO Director to issue directives that establish uniform standards for safeguarding; security education and training; agency self-inspections; and classification and declassification guides.	Establishes a system designed to result in cost savings through uniformity and the application of reasonable risk management principles.
<i>Policy Advisory Council</i>	No comparable provision.	Establishes an Information Security Policy Advisory Council consisting of Government and Non-Government representatives.	Provides a forum for interested organizations outside the Government to express their concerns about the system and to interact with those responsible for the system within Government.
<i>Accountability of Top Management</i>	No comparable provision.	Requires heads of agencies to demonstrate personal and senior management commitment for the effective implementation of the program.	Remedies a major shortfall in the current system by emphasizing the role and responsibility of senior management for the success of the program, rather than simply delegating the onus to non-policy security officials.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993**

PART 5 OF DRAFT ORDER

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Individual Accountability</i>	No comparable provision.	Requires that the performance contracts of critical personnel, including classifiers and security professionals, include the management of classified information as an element of performance to be evaluated annually.	Increases individual accountability for the effectiveness of the system by tying its management to the performance contracts or plans of its most important implementers, including original classifiers.
<i>Accounting for Costs</i>	No comparable provision.	Requires agencies to account for all costs associated with the security classification program and to submit those costs annually to ISOO for publication.	Enables the executive branch to account for the costs of the classification system, rather than simply speculate, as a means of cost control.
<i>Sanctions</i>	No comparable provision.	Requires sanctions when an individual creates or continues a special access program contrary to the requirements of the Order.	Establishes a further control mechanism to prevent the creation or continuance of unnecessary special access programs.
<i>Sanctions</i>	No comparable provision.	Requires the prompt removal of classification authority from an individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of the Order.	Seeks to remedy the current situation in which, despite the general reference to sanctions for improper classification, such sanctions never seem to be imposed. Requires the prompt removal of classification authority while other sanctions are considered.

**COMPARISON OF MAJOR FEATURES OF E.O. 12356
AND DRAFT ORDER DATED AUGUST 17, 1993
PART 5 OF DRAFT ORDER**

FEATURE	E.O. 12356	DRAFT ORDER DATED AUGUST 17	IMPROVEMENTS
<i>Establishment of an Inter-agency Security Classification Appeals Panel</i>	No comparable provision	Establishes an Interagency Security Classification Appeals Panel responsible for deciding appeals of final agency decisions of (i) mandatory declassification review requests, and (ii) challenges to classification.	Allows for independent review of final agency decisions in the areas of classification challenges and declassification reviews.
<i>Role of Agency Inspector General</i>	No comparable provision.	Calls for the Inspector General to conduct periodic audits of the implementation and administration of the program.	Reinforces within agencies the need for internal oversight. Provides for more comprehensive reviews of implementation of the program.

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: _____

HOW DECLASSIFICATION WORKS: DRAFT EXECUTIVE ORDER OF AUGUST 17, 1993

Information classified SECRET under this Order

A. If less than 25 years old	B. If over 25 years old	C. If over 40 years old
1. If marked with a date or event for declassification, automatically declassified at that date or event.	1. If of permanent historical value, may be declassified in the course of a systematic declassification review conducted by the agency of origin, or by the National Archives with respect to information in the Archivist's custody and control.	1. Automatically declassified.
2. Otherwise, automatically declassified ten years from the date of classification.		2. May remain classified only if the agency head exempts specific information that falls within one of four narrow categories, and provides written justification to the ISOO Director at least 180 days before the information is to be automatically declassified. Director may reject the extension. Agency head may appeal to NSC.
3. May remain classified for a longer period, not to exceed ten additional years if, no earlier than 180 days before the date of automatic declassification, an original classifier extends the classification in accordance with the original classification standards of the Order.	NOTE: In addition to the foregoing processes, information may be declassified at any time during its life span as the result of a declassification review, conducted at the agency's initiative or in response to a Freedom of Information Act or mandatory review request or appeal.	

HOW DECLASSIFICATION WORKS: DRAFT EXECUTIVE ORDER OF AUGUST 17, 1993

Information classified TOP SECRET under this Order		
A. If less than 25 years old	B. If over 25 years old	C. If over 40 years old
1. If marked with a date or event for declassification, automatically declassified at that date or event.	1. If of permanent historical value, may be declassified in the course of a systematic declassification review conducted by the agency of origin, or by the National Archives with respect to information in the Archivist's custody and control.	1. Automatically declassified.
2. Otherwise, automatically declassified 15 years from the date of classification.		2. May remain classified only if the agency head exempts specific information that falls within one of four narrow categories, and provides written justification to the ISOO Director at least 180 days before the information is to be automatically declassified. Director may reject the extension. Agency head may appeal to NSC.
3. May remain classified for a longer period, not to exceed ten additional years if, no earlier than 180 days before the date of automatic declassification, an original classifier extends the classification in accordance with the original classification standards of the Order.	NOTE: In addition to the foregoing processes, information may be declassified at any time during its life span as the result of a declassification review, conducted at the agency's initiative or in response to a Freedom of Information Act or mandatory review request or appeal.	

HOW DECLASSIFICATION WORKS: DRAFT EXECUTIVE ORDER OF AUGUST 17, 1993

Information classified CONFIDENTIAL under a prior Order		
A. If less than 25 years old	B. If over 25 years old	C. If over 40 years old
1. If marked with a date or event for declassification, automatically declassified at that date or event.	1. If of permanent historical value, may be declassified in the course of a systematic declassification review conducted by the agency of origin, or by the National Archives with respect to information in the Archivist's custody and control.	1. Automatically declassified no later than two years from the issuance of the Order.
2. If marked "OADR," automatically declassified six years from the issuance of the Order.		2. May remain classified only if the agency head exempts specific information that falls within one of four narrow categories, and provides written justification to the ISOO Director at least 180 days before the information is to be automatically declassified. Director may reject the extension. Agency head may appeal to NSC.
3. May remain classified for a longer period if, no earlier than 180 days before the date of automatic declassification, an original classifier classifies the information Secret in accordance with original classification standards of the Order.	NOTE: In addition to the foregoing processes, information may be declassified at any time during its life span as the result of a declassification review, conducted at the agency's initiative or in response to a Freedom of Information Act or mandatory review request or appeal.	

HOW DECLASSIFICATION WORKS: DRAFT EXECUTIVE ORDER OF AUGUST 17, 1993

Information classified SECRET under a prior Order		
A. If less than 25 years old	B. If over 25 years old	C. If over 40 years old
1. If marked with a date or event for declassification, automatically declassified at that date or event.	1. If of permanent historical value, may be declassified in the course of a systematic declassification review conducted by the agency of origin, or by the National Archives with respect to information in the Archivist's custody and control.	1. Automatically declassified no later than two years from the issuance of the Order.
2. If marked "OADR," automatically declassified 10 years from the issuance of the Order.		2. May remain classified only if the agency head exempts specific information that falls within one of four narrow categories, and provides written justification to the ISOO Director at least 180 days before the information is to be automatically declassified. Director may reject the extension. Agency head may appeal to NSC.
3. May remain classified for a longer period not to exceed ten additional years if, no earlier than 180 days before the date of automatic declassification, an original classifier extends the classification in accordance with the original classification standards of the Order.	NOTE: In addition to the foregoing processes, information may be declassified at any time during its life span as the result of a declassification review, conducted at the agency's initiative or in response to a Freedom of Information Act or mandatory review request or appeal.	

HOW DECLASSIFICATION WORKS: DRAFT EXECUTIVE ORDER OF AUGUST 17, 1993

Information classified TOP SECRET under a prior Order		
A. If less than 25 years old	B. If over 25 years old	C. If over 40 years old
1. If marked with a date or event for declassification, automatically declassified at that date or event.	1. If of permanent historical value, may be declassified in the course of a systematic declassification review conducted by the agency of origin, or by the National Archives with respect to information in the Archivist's custody and control.	1. Automatically declassified no later than two years from the issuance of the Order.
2. If marked "OADR," automatically declassified 15 years from the issuance of the Order.		2. May remain classified only if the agency head exempts specific information that falls within one of four narrow categories, and provides written justification to the ISOO Director at least 180 days before the information is to be automatically declassified. Director may reject the extension. Agency head may appeal to NSC.
3. May remain classified for a longer period if, no earlier than 180 days before the date of automatic declassification, an original classifier extends the classification in accordance with the original classification standards of the Order.	NOTE: In addition to the foregoing processes, information may be declassified at any time during its life span as the result of a declassification review, conducted at the agency's initiative or in response to a Freedom of Information Act or mandatory review request or appeal.	