

John,

This is yet another version for your consideration. It would give the Security Policy Board the responsibility to write the directives concerning physical security only, but these directives would be issued by OMB. ISOO would write all of the other directives for the EO, and these directives would also be issued by OMB. ISOO stays at OMB; NSC gives ISOO policy guidance. This carves up the baby in a way that gives everyone something, but probably satisfies no one completely.

George asks that you run the meeting today!


Gina

95 MAR 27 P 3: 41

→
→
→
policy guidance
[SPB]

Mar 27
4:00pm
Rm 300
HOLD
E.O. Declass.

Program
Section 5.2 ~~Policy~~ Direction.

(a) The National Security Council shall provide overall policy guidance for the program established by this Order.

(b) The Director of the Office of Management and Budget shall be responsible for implementing and monitoring the program established by this Order, and for issuing such directives as are necessary to implement this Order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

- ~~(1) safeguarding classified information;~~
- (2) agency security education and training programs;
- (3) agency self-inspection programs;
- (4) classification and declassification guides; and
- ~~(5) implementing the authorities of the Information Security Oversight Office.~~

(c) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) sec. Policy Bd

Section 5.3 Information Security Oversight Office; Security Policy Board

(a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs, shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget and in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop the directives prescribed in Section 5.2(b)(2) through (5) of this order;

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

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected

agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval through the Director of the Office of Management and Budget;

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

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

(c) The Security Policy Board, established by Presidential Decision Directive ~~28~~, shall develop the directive on

 safeguarding classified information prescribed in Section 5.2(b)(1) of this order. This directive shall pertain to the processing, handling, storage, distribution, transmittal and destruction of and accounting for classified information.

NATIONAL SECURITY COUNCIL

WASHINGTON, D.C. 20506

March 24, 1995

John,

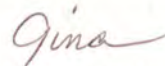
A few items:

1. Attached (tab I) is the version we discussed yesterday which places ISOO within OMB, gives NSC policy direction over ISOO, and does not mention the Security Policy Board (SPB). However, I think the omission of the SPB and the specific role it should play in writing uniform standards for safeguarding classified information, agency security education and training programs, classification and declassification guides, and agency self-inspection programs is problematic. By not carving out a role for the SPB specifically, OMB will assert the authority to do so, since the order gives OMB the authority to issue the implementing regs for the order. The second attached version (tab II) includes the SPB (in italics and bold).

2. At tab III is the SPB's version of sections 5.2 and 5.3, which will essentially give them the authority to execute this order, and leave ISOO with an undefined "oversight" role. Also attached -- if you have not already seen it -- is Aftergood's latest piece blasting the SPB and the order (tab IV).

3. I just learned that Alice Rivlin testified before the House Appropriations Committee and the issue of ISOO was raised. She stated her view that it should be moved to NARA and the Committee concurred. It appears that in the absence of some action from the Executive Branch to reverse this (or fierce opposition from the Senate develops), we should probably expect the Congress to move ISOO to NARA.

4. The meeting to discuss sections 5.2 and 5.3 is scheduled for Monday at 4:00 PM with Sally Katzen, Bob Damus, George, Mort, you and me. We were unable to get all principals together Friday.



Gina Genton

Attachments

Tab I	Places ISOO within OMB
Tab II	Includes SPB
Tab III	SPB's version
Tab IV	Secrecy & Government Bulletin

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.

TAB I

Divider Title: _____

Section 5.2 Policy Direction.

(a) The National Security Council shall provide overall policy guidance for the program established by this order.

(b) The Director of the Office of Management and Budget shall be responsible for implementing and monitoring the program established by this order, and for issuing such directives as are necessary to implement this order. These directives shall be binding upon the agencies. The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

Section 5.3 Information Security Oversight Office.

(a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs, shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget, and in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) issue and publish a directive, which shall be binding on the agencies, that implements the authorities of the Information Security Oversight Office as provided in this order;

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

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval through the Director of the Office of Management and Budget;

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

(7) report at least annually to the President on the implementation of this order; and

(8) convene and chair interagency or other meetings to discuss matters pertaining to the program established under this order

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.

TAB II

Divider Title: _____

VERSION WITH THE SECURITY POLICY BOARD

Section 5.2 Policy Direction.

(a) The National Security Council shall provide overall policy guidance for the program established by this order.

(b) The Director of the Office of Management and Budget shall be responsible for implementing and monitoring the program established by this order, and for issuing such directives as are necessary to implement this order. These directives shall be binding upon the agencies. The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

Section 5.3 Information Security Oversight Office.

(a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs, shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget, and in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) issue and publish a directive, which shall be binding on the agencies, that implements the authorities of the Information Security Oversight Office as provided in this order;

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

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget,

who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval through the Director of the Office of Management and Budget;

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

(7) report at least annually to the President on the implementation of this order; and

(8) convene and chair interagency or other meetings to discuss matters pertaining to the program established under this order

(9) *review the instructions of the Security Policy Board, agency implementing regulations, and agency guides for systematic declassification review. The Director shall require any instruction, regulation or guide be consistent with the order and its implementing directives.*

(c) The Security Policy Board established by Presidential Decision Directive shall:

(1) issue instructions, which shall be binding on the agencies, that establish uniform standards for:

(A) Safeguarding classified information, to include the marking, use, processing, storage, reproduction, transmittal and destruction of such information;

(B) agency security education and training programs;

(C) agency self-inspection programs; and

(D) classification and declassification guides.

(2) prescribe and issue, after consultation with affected agencies, standardized forms that will promote the implementation of the program established under this order.

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.

TAB III

Divider Title: _____

Section 5.2 Policy Direction.

(a) The National Security Council shall provide overall policy guidance for the program established under this Order.

(b) The Director of the Information Security Oversight Office shall be responsible for ~~implementing the oversight~~ and monitoring of the program established under this Order.

(c) The Security Policy Board established by Presidential Decision Directive shall be responsible for formulating and implementing security policy for the program established under this Order.

Section 5.3 Information Security Oversight Office; Security Policy Board.

(a) There is established an Information Security Oversight Office.

(1) Remainder Reserved.

(b) The Director of the Information Security Oversight Office shall:

~~(1) issue and publish, with the concurrence of the National Security Council, a directive which shall be binding on the agencies., that implements the authorities of the Information Security Oversight Office as provided in this Order;~~

~~(2)~~ (21) oversee agency actions to ensure compliance with this Order and its implementing directives;

~~(3)~~ (32) review ~~the instructions of the Security Policy Board,~~ agency implementing regulations and agency guides for systematic declassification review. The Director shall require any ~~instruction,~~ regulation or guide to be changed if inconsistent with this Order or its implementing directives. Any such decision by the Director may be appealed to the

National Security Council. The instruction, regulation or guide shall remain in effect pending a prompt decision on the appeal;

(43) have the authority to conduct on-site reviews of each agency's program established under this Order, and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the deal of access to the National Security Council within 60 days of the Director's request for access. Access shall be denied pending a prompt decision by the National Security Council;

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

(65) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

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

(87) have the authority to convene and chair interagency or other meetings to discuss matters pertaining to the program established under this Order.

(c) The Security Policy Board shall:

(1) issue and publish, subject to the approval of the National Security Council, directives instructions, for the implementation of this Order which shall be binding on the agencies, that establish uniform standards for:

(A) Safeguarding classified information, to include the marking, use, processing, storage, reproduction, transmittal and destruction of such information;

(B) agency security education and training programs;

(C) agency self-inspection programs; and

(D) classification and declassification guides.

(2) prescribe and issue, after consultation with affected agencies, standardized forms that will promote the implementation of the program established under this Order.

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.

TAB IV

Divider Title: _____

Federation of American Scientists
307 Massachusetts Avenue, NE
Washington, D.C. 20002

for more information:
Steven Aftergood
(202)675-1012
saftergood@igc.apc.org

SECRECY & GOVERNMENT BULLETIN

To Challenge Excessive Government Secrecy and
To Promote Public Oversight and Free Exchange
In Science, Technology, Defense, and Intelligence

Issue No. 46
March-April 1995
ISSN 1061-0340

Security Policy Board Delays New Exec Order

An attempt by the CIA-dominated Security Policy Board (SPB) to seize control of all secrecy policy is the latest obstacle to completion of the long-delayed executive order establishing a new classification system.

President Clinton called for a new classification system in his Presidential Review Directive 29, dated April 26, 1993. Information Security Oversight Office (ISOO) director Steven Garfinkel acknowledged with some chagrin that nearly two years have passed since then, and yet the new order is still not finished.

"There is a remote possibility that we will celebrate [sic] the second anniversary without a new order, but we will not go much beyond that," Mr. Garfinkel said at a meeting at DOE headquarters on March 16. "No substantive issue remains to be decided. There is only a turf issue." Although he declined to elaborate, the turf issue in question is the SPB's attempt to take over the management of the classification system, a function that is currently exercised by ISOO.

The Security Policy Board was created last year by Presidential Decision Directive 29 to coordinate the nation's disparate security policies, which were widely perceived to be fragmented and incoherent.

But so far the SPB has been functioning like some wayward Eastern European bureaucracy, untainted by any hint of democratic principles or fair play. In a seeming violation of the Federal Advisory Committee Act, the SPB has invited defense industry lobbyists to participate actively in its deliberations while preventing other members of the public any access whatsoever. This is poor strategy since it needlessly antagonizes concerned citizens whose interests may not precisely coincide with those of defense contractors.

The National Security Council is taking the position that the SPB is a CIA-based entity and therefore exempt from the normal legal provisions for fair and equal access by all interested parties. And indeed, six of the Board's eighteen staff members are CIA employees, including staff director Peter Saderholm, who has been a CIA imagery analyst, staff officer, and collection manager. The NSC position in effect places the CIA in charge of all security-related policies government-wide.

The Electronic Privacy Information Center (EPIC), a Washington public interest group, filed a lawsuit against the NSC in early March, seeking access to SPB documents. EPIC is particularly concerned about the SPB's declared intention to assume responsibility for security of unclassified computer information systems--in apparent violation of the Computer Security Act of 1987, which assigned that responsibility to the National Institute of Standards and Technology.

"This is a battle over the accountability and oversight of government computer policy," said EPIC director Marc Rotenberg. "These decisions must be

made in the bright light of day."

The CIA says that a separate body called the Security Policy Advisory Board has been created specifically to represent "the non-governmental and public interest perspective." The appointees to that Advisory Board have not yet been named by the President. But the list of potential nominees that was sent to the White House did not include critics of government secrecy, civil libertarians or privacy activists. Instead, the SPB staff recommended that the public interest be represented by retired intelligence community officials and industry lobbyists.

The struggle over who will control the classification system is "a crisis for the security community," declared John Elliff, a senior Pentagon counterintelligence official who favors total SPB control of security policy. But it is also a crisis for concerned members of the general public. If the SPB gambit is successful, interested citizens could be effectively shut out of official security policy deliberations.

DOE Begins Fundamental Secrecy Review

As part of its ongoing Openness Initiative, the Energy Department has undertaken what it said is the first comprehensive examination of its classification policies in nearly fifty years. The Fundamental Classification Review will take a year to reevaluate the basis for classification of defense-related nuclear information "with the objective of promptly releasing all information no longer warranting such protection."

The review group, chaired by Dr. Al Narath of Sandia National Labs, will be comprised of some fifty experts mainly from government and the national labs. Seven working groups will focus on information in the categories of weapons science, weapons design, materials production, weaponization, weapons production and military utilization, military reactors, and safeguards and security. A DOE fact sheet on the initiative is available from S&GB.

At the first meeting of the review group on March 16, the need for a fundamental classification review was roundly endorsed by invited speakers from several public policy, nonproliferation, and environmental advocacy groups as well as government officials and prominent scientific figures.

Edward Teller called the DOE Openness Initiative "the most successful undertaking of the present Administration."

Dr. Teller, who for decades has taken an extreme position against secrecy, generally urged the review group to adopt a very short duration for classification. "I think there should be a time limit of five years. Maybe of two years. In principle, what is known today will be accessible to practically everybody who goes after it in a short time. And by stretching the time

limit, we only give ourselves an unrealistic view of the actual situation. So my suggestion to you is to consider, even in the dangerous areas of weapons, a short time period."

He did allow that some weapon design details should remain classified. "I am worried about design information when it goes into that kind of detail which I will need at least seven weeks to understand. But what is not hard to explain is not worth keeping secret."

Dr. Teller specifically urged "complete openness" concerning U.S. plutonium and tritium stockpiles, as well as the current size of the U.S. arsenal of nuclear weapons. ("I can tell you openly, we have more than we need," he said.)

Dr. Wolfgang Panofsky, who chairs the long-delayed National Academy of Sciences study on DOE classification policy (now expected in May), expressed his opinion that "very high fences should remain around truly important sensitive subjects, but that classification and dissemination restrictions on a large volume of less sensitive material should be removed entirely."

Dr. Panofsky also suggested that "DOE does not know very well how big their job really is." He noted that last year's estimate of a backlog of 32 million pages awaiting declassification review has recently been revised upward to 130 million pages.

Congress Permits "Unwise" Covert Actions

Congressional oversight of covert action has failed to screen out programs that are "unwise" and inappropriate, says a former CIA official. The failure of existing covert action oversight mechanisms dictates that an "external" non-governmental review process should be established, according to David Gries, who retired from the CIA in 1994 after 33 years in intelligence operations and analysis.

Mr. Gries presented his views in an article entitled "A New Look for Intelligence" in the British academic journal *Intelligence and National Security*, vol. 10, no. 1, January 1995, pp. 170-183.

"Since the late 1970s, the [intelligence] community has employed elaborate internal review procedures for covert actions requested by policymakers, and the National Security Council and Congressional intelligence committees have required equally rigorous reviews," Mr. Gries noted. Nevertheless, "Despite these measures, a small number of unwise and unworkable covert action plans continue to gain intelligence community support as well as presidential and Congressional approval. These lapses argue strongly for external review."

Mr. Gries asserted that spending on covert action has been reduced to less than one percent of the intelligence community's budget. Still, "To assure that the remaining covert actions are truly needed and do not violate basic American values, the intelligence community-- or at least CIA, which is responsible for conducting covert action at the direction of the President-- should consider seeking advice from experts outside government before asking the President and Congress to authorize and fund new operations."

Although Mr. Gries did not specify which covert actions he believes should have been blocked by Congress, it is difficult to doubt the basic validity of his criticism, particularly since he is not a "dissident" seeking absolution for his sinful past.

On the other hand, it is easy to question the value of his proposed solution. Even if another "advisory committee" were set up, neither the intelligence community nor Congress would be likely to tolerate meaningful external review on an ongoing basis.

In any event, few alert Americans look to Congress anymore for serious intelligence oversight, due to its failure to end unnecessary budget secrecy, as well as its handling of the NRO building fiasco and other delinquencies. For better or worse, the most important

intelligence oversight is now being done by a small corps of investigative journalists and national security reporters, notably at the *New York Times* and the *Washington Post*. In an implicit confirmation of their growing impact, Acting CIA Director Studeman has recently written letters to the editor at both the *Times* (3/4/95) and the *Post* (3/17/95), taking exception to some recent news reports.

Spysat Secrecy Needs to Be Overcome

The secrecy surrounding spy satellite programs is preventing an accurate official assessment of their vulnerability and hindering the adoption of needed structural reforms, according to a newly published study.

"The organizations and practices which grew up around national security space systems during the Cold War are now a serious impediment to analyzing and meeting the challenges which will face us in the coming years and decades," writes Allen Thomson in "Satellite Vulnerability: A Post-Cold War Issue?" published in the journal *Space Policy*, vol. 11, no. 1, February 1995. The author served as a CIA analyst from 1972 to 1985.

Mr. Thomson writes that excessive secrecy in the spysat field has become a "full-blown organizational dysfunction," preventing a full understanding by policymakers of the growing vulnerability of spy satellites and the options for restructuring the overhead reconnaissance program. This secrecy needs to be substantially reduced, he argues.

"At a minimum," Thomson writes, "the special 'security' channels and compartments associated with overhead reconnaissance should be reexamined, the principal missions and characteristics of reconnaissance satellites declassified, and planning for future systems opened to general discussion and critique, much as is the case for other weapons systems."

Mr. Thomson's paper was reviewed and approved for publication by the CIA, as required. However, the National Reconnaissance Office attempted to block release of the paper, delaying its publication for more than a year.

Hot Documents

- A March 2 draft of the pending executive order on Access to Classified Information (security clearances) is a marked improvement over earlier drafts generated by the secretive Security Policy Board (S&GB 45). For the first time, the order would grant government employees whose clearance is denied or revoked an opportunity to appear personally before an adjudicative panel, along with other modest improvements in due process. Available from S&GB for \$2 or a kind word.

- A report prepared for the DOE Office of Counterintelligence takes a close look at the difficulties of protecting economically valuable information from foreign collection at government laboratories. "A Vulnerability Assessment: Protecting Key Technologies at Los Alamos National Laboratory" (November 1994) contains some interesting case studies and thoughtful analysis. "The openness of investigation in the United States may be the key to development of many fertile areas. Other countries that shepherd their research and protect it may hamper its ultimate development. No wonder so many countries turn to the United States for ideas to turn into products!" On the other hand, "The Internet, which is accessible worldwide, is starting to be a major vulnerability." And, says the counterintelligence report, "A lot of good science is at risk from FOIA." A copy of the unreleased report (marked "official use only") is available from S&GB for \$5. US citizens only.

Secrecy & Government Bulletin is written by Steven Aftergood. This publication may be freely reproduced.

BACKGROUND PAPER
PUBLIC INTEREST BALANCING TEST

File.
E.O. Classification

At issue is whether agencies should be required to balance the public interest in disclosure against the possible harm to national security in deciding whether to declassify information (known as the "back-end" public interest balancing test) and whether that decision should be subject to court review under the Freedom of Information Act (FOIA).

The FOIA provides that information may be withheld if it is properly classified pursuant to an Executive Order. Persons seeking documents under the FOIA can challenge a decision to withhold in a lawsuit and the court makes a de novo interpretation as to whether the information fits within the exemption. Thus, whatever standard for declassification is written into the Executive Order becomes the standard for judicial review in an FOIA lawsuit.

The Department of Justice, which defends all FOIA cases in court, is the principal opponent of the balancing test, but virtually all other agencies would be inclined to support Justice's view. Justice believes the balancing test should be deleted from the Order or at a minimum rewritten so that the Government can argue it is not subject to judicial review. Its argument is that there will be an added burden of defending withholding information based on the argument that the public value of the information outweighs the harm to national security and that a court might order the withholding of information that the government wanted to keep secret. In other words, the courts will look to the factual basis behind application of the test which will impose additional requirements on officials who prepare and sign declarations. (See attached memorandum from the Attorney General for a detailed explanation of Justice's views and proposed alternative language.)

Proponents of the balancing test argue it is one of the most important reforms in the Order and one of great value to the public interest community and the press. It reflects a commitment to openness and to the view that the public value of information should be taken into account in deciding whether to release information. Removing the balancing test, or rewriting it to prohibit judicial review would be seen as an enormous step backward in disclosure policy. (The Carter Order had a balancing test, but the government proceeded to argue that it was not subject to judicial review. The courts agreed.)

A balancing test subject to judicial review will increase the burden of defending FOIA cases. However, it can also be argued that this is a necessary and acceptable cost to force agencies to consider the public value of information before deciding whether to release information requested under the FOIA. Proponents believe that the only effective way to impose that process on the bureaucracy is to make it a part of the Executive Order which is subject to judicial review. If judicial review is not available, agencies are unlikely to take the requirement seriously.

Proponents of the balancing test also maintain that there is no real danger that information would be ordered released by the courts which the President or senior officials do not believe should be disclosed. Courts have been and will continue to be extraordinarily deferential to executive branch judgments about national security. In fact, no court has ever issued a final order directing the release of information which the government argued was properly classified. Proponents believe judges would defer to the affidavit of a senior government official that, even taking account of the public value, the information should remain classified. A tentative decision by a District Court judge to order disclosure would always be subject to a motion to reconsider or to stay pending appeal. Thus, there will always be an opportunity to provide a more persuasive affidavit from a more senior official or even to invoke Executive Privilege.



Office of the Attorney General
Washington, D. C. 20530

June 30, 1994

MEMORANDUM FOR: THE ASSISTANT TO THE PRESIDENT
FOR NATIONAL SECURITY AFFAIRS
THE COUNSEL TO THE PRESIDENT

FROM: THE ATTORNEY GENERAL *[Signature]*

SUBJECT: Proposed Executive Order on National Security Information

The Deputy Attorney General's April 20, 1994 Memorandum for the Assistant to the President for National Security Affairs (attached at Tab A) set forth three problems created by the draft Executive Order on classified national security information: (1) the substantial logistical problems that the automatic declassification provisions pose for the FBI; (2) the litigation risks created by the balancing provisions; and (3) the litigation risks posed by the "reasonable doubt" provisions. That Memorandum also proposed specific alternatives to these provisions that would ameliorate these problems.

On May 24, a group of DoJ and FBI representatives met with representatives of the NSC to discuss these problems and the proposed solutions. Since that meeting, the FBI has informally proposed several options that would mitigate the logistical problems posed by the declassification provisions. It is my understanding, however, that this issue remains unresolved.

The other two problems also have not been resolved. If left in their current form, the public interest balancing test and reasonable doubt provisions would make it more difficult for the Department of Justice to defend Executive Branch classification decisions. These provisions would invite courts to substitute their judgment for that of the Executive in matters affecting national security. Accordingly, we continue to believe that these provisions should be deleted from the draft order or, in the alternative, revised in the manner discussed in the Deputy Attorney General's April 20 Memorandum and in this Memorandum.

I understand the sentiment that the increased judicial scrutiny that would be occasioned by these provisions is desirable, because it would discourage excessive classification and encourage declassification, thereby promoting openness in government. But the Administration's new FOIA policy, set forth in statements by the President and by me last October, and its government-wide access initiatives do a great deal to promote

openness in government. Executive agencies should be given the chance to make this commitment to openness work before their classification and declassification decisions are subjected to additional review by courts.

More importantly, the draft order already provides administrative procedures to check significant over-classification, including: (1) the Interagency Security Classification Appeals panel, which will review appeals of decisions denying requests for mandatory declassification; (2) the Information Security Oversight Office, which is empowered to conduct on-site reviews of agencies' classification programs; (3) the requirement that agencies establish and maintain self-inspection programs to review and assess their classified product; and (4) the requirement that each agency's Inspector General also conduct periodic evaluations of the agency's classification program. In light of these procedures, heightened judicial scrutiny of Executive Branch decisions in this area should be unnecessary and, as discussed below, may well have undesirable results.

I. THE PUBLIC INTEREST BALANCING TEST

A. The Draft Order

As currently drafted, section 3.2(b) of the draft Executive Order provides:

If an agency head or senior agency official determines that the public interest in disclosure of specific information classified by that agency outweighs the national security interest in its continued classification, the information shall be declassified even though it continues to meet the standards for classification under this Order.¹

As discussed in the Deputy Attorney General's April 20 Memorandum, this provision could undermine the Department's ability successfully to defend Executive Branch classification decisions. Although courts traditionally have deferred to the Executive's judgment concerning whether disclosure of information would damage national security, it is our fear that courts could decide that the Executive Branch has no special expertise in assessing the "public interest" in disclosure, and therefore might accord an agency's application of the balancing test little deference. The addition of this "public interest" factor, then,

¹ Section 1.2(b) of the draft order provides for a similar balancing test at the initial classification stage. The NSC has informed us, however, that section 1.2(b) will be deleted from the order.

may invite courts to substitute their judgment for Executive Branch judgments. This result would be inconsistent with the Executive's constitutional responsibility to protect national security information.

Moreover, even if courts in the end upheld the Executive's decisions, the addition of the balancing test provision is predicted to encourage litigation challenging particular applications of that provision, requiring depositions, detailed affidavits, production of deliberative documents, and possibly trials. This new litigation could pose a significant burden on both the Department and on the affected client agencies. We therefore continue to believe that the public interest balancing test should be deleted from the draft Executive Order.

B. The Carter Administration Order

It has been suggested that reinstating the balancing test provision of the Carter Administration's Executive Order (E.O. 12065) in lieu of the draft order's provision might ameliorate some of these problems. The balancing provision of the Carter order (section 3-303) was substantially similar to section 3.2(b) of the draft order. It provided:

It is presumed that information which continues to meet the classification requirements in Section 1-3 requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head, a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order, an official with Top Secret classification authority, or the Archivist of the United States in the case of material covered in Section 3-503. That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

(Emphases added.)

This provision was arguably slightly more protective of the Executive's prerogative in protecting national security information than the draft order. For example, the statement that properly classified information is "presumed" to require continued protection and the limitation of balancing to "some cases" permitted the Department to argue that balancing was not mandatory in all cases, but only in exceptional cases in which the relevant agency official determined, in his or her discretion, that balancing was appropriate.

Significantly, though, the Carter Administration concluded that this provision, standing alone, was insufficiently protective of governmental interests. For that reason, a Memorandum was issued by then-National Security Adviser Zbigniew Brzezinski stressing the discretionary nature of the balancing test. That Memorandum (attached at Tab B) emphasized that the balancing test did not apply to all declassification decisions, but only in "exceptional" and "rare" cases. It also specifically stated that the provision was "not intended to modify the substantive criteria or procedures for classification," but simply "reflect[ed] th[e] Administration's policy that properly classified information nevertheless may be declassified under some circumstances." Finally, the Brzezinski Memorandum made clear that the balancing test was a "discretionary determination[]." See, e.g., Salisbury v. United States, 690 F.2d 966 (D.C. Cir. 1982) (relying in part on Brzezinski Memorandum in holding that balancing test was discretionary).

Even with the Brzezinski Memorandum, however, the Carter order's language prompted litigation over a host of issues, including: (1) whether balancing of the public interest was mandatory or discretionary; (2) whether an agency's failure to balance or its assessment of the national security/public interest balance was subject to judicial review; (3) if judicial review was available, whether the agency's decision should be accorded deference or reviewed de novo; and (4) whether the "public interest" had to be considered at the initial classification stage as well as the declassification stage.²

Circumstances with regard to FOIA litigation have changed dramatically since the Carter Administration. There is far more litigation under FOIA in general today, and the FOIA requester community and bar are more specialized and sophisticated than they were in the late 1970s and early 1980s. As a result, reinstating the Carter order's balancing test would engender considerably more litigation today than E.O. 12065 did during the

² See e.g., McGehee v. Casey, No. 81-0734 (D.D.C. Sept. 25, 1981), 718 F.2d 1137 (D.C. Cir. 1983); Afshar v. Dept. of State, 76-1421 (D.D.C. Oct. 24, 1980), aff'd in part, vac'd in part, rev'd in part and remanded, 702 F.2d 1125 (D.C. Cir. 1983); Halkin v. Helms (Halkin II), 690 F.2d 977 (D.C. Cir. 1982); Salisbury v. United States, No. 80-909 (D.D.C. April 14, 1981), aff'd, 690 F.2d 966 (D.C. Cir. 1982); Allen v. CIA, 636 F.2d 1287 (D.C. Cir. 1980), on remand, 516 F. Supp. 653 (D.D.C. 1981); Andres v. CIA, No. 80-0865 (D.D.C. April 28, 1981), rev'd and remanded, 673 F.2d 550 (D.C. Cir. 1981) (table) (unpublished); Marks v. Casey, No. 77-1108 (D.D.C. July 28, 1981); Patterson v. CIA, No. 78-0070 (D.D.C. Feb. 5, 1981); Ground Saucer Watch, Inc. v. CIA, No. 78-859 (D.D.C. May 10, 1980); Kanter v. Dept. of State, 479 F. Supp. 921 (D.D.C. 1979).

C. Options

1. No Public Interest Balancing Test. For the reasons set forth above and in the Deputy Attorney General's April 20 Memorandum, the Department of Justice continues to recommend that the public interest balancing test be deleted from the draft order. Any balancing test, even if accompanied by language emphasizing the discretionary nature of the test, will increase the amount of litigation challenging declassification decisions. Moreover, inclusion of a balancing test could undermine judicial deference to the Executive's determinations in this area.

2. Carter "Plus." As noted in the April 20 Memorandum, if some form of balancing test is desired, there should be an explicit statement that balancing is an exercise of Executive Branch discretion and does not create any rights subject to judicial review, just as the Brzezinski Memorandum made it explicit that the balancing test under the Carter order was discretionary. The Administration's position would be consistent with, but clearer than, the Carter order and would represent how the Carter order was, in fact, implemented. The Carter order could be revised as follows (with the revisions in boldface):

It is presumed that information that continues to meet the classification requirements under this Order requires continued protection. In some **exceptional** cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order. That official will determine, **as an exercise of discretion**, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

This provision does not amplify or modify the substantive criteria or procedures for classification, and does not create any substantive or procedural rights subject to judicial review.³

³ My October 4, 1993 Memorandum for Heads of Departments and Agencies encouraging the use of "discretionary disclosures" under FOIA contained a similar disclaimer: "[T]his policy is not

DRAFT

ACTION

MEMORANDUM FOR THE PRESIDENT

FROM: ANTHONY LAKE
JOHN PODESTA
GEORGE STEPHANOPOULOS

SUBJECT: Proposed Executive Order on National Security Information

Purpose

To decide whether to require a judicially reviewable public interest balancing test when agencies decide whether to declassify information and whether to require the declassification of almost all government documents at 25 years.

Background

We have been working on a revised executive order on the classification and declassification of information for over a year. We felt the draft Executive Order submitted by the 26-member interagency task force established by Presidential Review Directive 29 did not achieve your goal of more open and accountable government. Consequently, this draft was substantially reworked by the NSC staff. Tony Lake subsequently authorized the dissemination of a new draft Order to executive branch agencies for comment last month.

NSC staff has reviewed these comments and made a number of changes to the draft to accommodate some agency concerns. However, there are two major items we believe you should decide on now, prior to the release of the draft Executive Order to OMB for formal coordination. These include: (1) whether agencies should be required to weigh the public interest in disclosure against the possible harm to national security in deciding whether to declassify information and whether that decision should be subject to court review under the Freedom of Information Act; and (2) whether documents should be subject to automatic declassification at 25 years. We believe it is important that you decide on these key elements before final OMB coordination with Executive Branch agencies, since it will be very difficult to retreat from these provisions once the Order is released to agencies and the public for formal comment.

Commensurate with the OMB process, a notice will be published in the Federal Register announcing the availability of a copy of the draft Order. The draft Executive Order would be sent to public interest groups as well as relevant Congressional Committees for their review and comment. This is consistent with the way both the Reagan and Carter Orders were handled.

Public Interest Balancing Test

DRAFT

The first issue that needs your decision now is whether the Executive Order should require agencies to balance the public interest in disclosure against the possible harm to national security in deciding whether to declassify information (known as the balancing test) and whether that decision should be subject to court review under the Freedom of Information Act (FOIA).

A word of explanation is required. The FOIA provides that information may be withheld if it is properly classified pursuant to an Executive Order. Persons seeking documents under the FOIA can challenge a decision to withhold in a lawsuit and the court makes a *de novo* interpretation as to whether the information fits within the exemption. Thus, whatever standard for declassification is written into the Executive Order becomes the standard for judicial review in an FOIA lawsuit.

The draft order, as it was circulated to the agencies, requires a balancing test both at the time of classification and when a declassification request is made. We are now planning to remove the requirement for balancing at the front end, but to leave in the requirement to balance when doing a declassification review and to make that judgment subject to the FOIA.

The only agency to raise objections to this is the Department of Justice which defends all FOIA cases in court. Justice wants the balancing test removed or at a minimum rewritten so we can argue it is not subject to judicial review. Its argument is that there will be an added burden of defending withholding information based on the argument that the public value of the information outweighs the harm to national security and that a court might order the withholding of information that the government wanted to keep secret.

Our response is that the balancing test is one of the most important reforms in the Order and one of great value to the public interest community and the press. It reflects your commitment to openness and to the view that the public value of information should be taken into account in deciding whether to release information. Removing the balancing test, or rewriting it to prohibit judicial review would be seen as an enormous step backward in disclosure policy. (The Carter Order had a balancing test, but the government proceeded to argue that it was not subject to judicial review.)

We agree with Justice that including a balancing test subject to judicial review will increase the burden of defending FOIA cases. However, we view this as a necessary and acceptable cost to force agencies to consider the public value of information before deciding whether to release information requested under the FOIA. The only effective way for you to impose that process on the bureaucracy is to make it a part of the Executive Order which is subject to judicial review. If judicial review is not available, agencies will not take the requirement seriously.

At the same time, we think there is no real danger that information would be ordered released by the courts which you or senior officials do not believe should be disclosed. Courts have been and will continue to be extraordinarily deferential to executive branch judgments about national security. In fact, no court has ever issued a final order directing the release of information which the government argued was properly classified. We think that judges would defer to the affidavit of a senior government official that, even taking account of the public value, the information should remain classified. A tentative decision by a District Court judge to order disclosure would always be subject to a motion to reconsider or to a stay pending appeal. Thus, there will always be an opportunity to provide a more persuasive affidavit from a more senior official or even to invoke Executive Privilege.

Automatic Declassification of Documents 25 Years Old

The draft Executive Order would be the first to establish automatic declassification or a "drop dead" date for previously classified information. As a practical matter, unless we go to a system which does away with line-by-line and document-by-document review, we will never be able to address effectively the hundreds of millions of pages of classified material awaiting review. The draft Order, as it has been circulated to the agencies, would require that any records over 25 years old be automatically declassified. (This means it would be made available to the public pursuant to a Freedom of Information Act request.) A document could be exempted from automatic declassification at the end of 25 years only by the head of the agency and only if the information fell into one of seven very narrow categories:

1. Reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method.
2. Reveal information that would assist in the development or use of weapons of mass destruction.
3. Reveal information that would impair US cryptologic systems or activities.
4. Reveal information that would impair the application of state of the art technology within a US weapon system.
5. Reveal actual US military war plans that remain in effect.
6. Reveal information that would cause exceptionally grave damage to the relations between the US and a foreign government.
7. Violate a statute, treaty, or international agreement.

It is our expectation that only a very small percentage of documents would require continued classification.

Most agencies favor a 30 year (instead of 25 year) "drop dead" date for the declassification of records for a number of reasons: it would reduce the immediate drain on agency resources for the review of older records; documents that are 30 years old will be slightly less sensitive than documents 25 years old; a 30 year standard would be consistent with both the Federal Records Act which requires agencies to offer permanently valuable records to the National Archives when they become 30 years old, and with the State Department's Basic Authorities Act which requires the State Department to declassify certain records of historical value at 30 years.

Our response is that the Joint Security Commission (established by the DCI and Secretary of Defense last year to review our overall security system) recommended a 25 year "drop dead" date with similar exemption categories. In addition, the acting Archivist, in a letter to the Vice President pursuant to the National Performance Review, said that there are virtually no records over 25 years old that need to remain classified on national security grounds.

While all agencies now concede they do not oppose automatic declassification in principle, they will claim they do not have the resources to carry out the Order and thus the USG risks disclosing information damaging to the national security. While making the threshold for automatic declassification at 30 years instead of 25 years would make some difference in cost, that difference is at the margin and we do not believe cost should drive your decision on this matter.

We recommend you support automatic declassification at 25 years. Agencies do not have problems with the concept of automatic declassification; cost is their real concern. Increasing the automatic declassification time frame would be seen as a significant retreat in disclosure policy.

Implementation Costs

The most costly element of the proposed Executive Order is declassifying the enormous backlog of documents that are 25 years old or older. The draft Executive Order gives agencies five years to clear the backlog. At the end of that period, documents would be declassified whether or not they had been reviewed. No one knows the real size of the backlog, but it is conservatively estimated at over a billion pages. According to preliminary figures compiled by the DCI, it will cost the USG on the order of \$100 million per year for five years to address the backlog.

The DCI has argued that implementation costs could be reduced by one-third if agencies were permitted to keep entire documents classified if the document contained any information that qualified for continued protection beyond 25 years. We believe this would undermine fundamentally the principle of automatic declassification -- the centerpiece of the proposed Executive Order -- and subject the Order to severe criticism by public interest groups.

We want to stress that the cost estimates are soft. For example, the FBI's estimates have changed by a factor of ten over the course of several weeks, and it believes it will be hard pressed to find the resources to conduct a thorough review of its documents. Agencies will have to develop a "risk management" methodology to review their documents, and may find it will cost less -- or more -- than these current rough estimates. While the cost is not trivial, when considered against what the government spends to maintain the current security system, estimated at \$16 billion annually, we believe it is worth dedicating the necessary funds now to address the backlog. No one has faced up to the problem in the past, and it will only become increasingly insurmountable as time passes. What is equally important is that we put in place a system prospectively in which documents are marked in such a way that declassification is truly automatic and done at minimal cost to the Government. This, too, is called for in the draft Order.

There undoubtedly will be a cost to the Government to declassify old records, but we believe the cost does not outweigh the benefit of public access to and confidence in the workings of its government.

Security Oversight Structure

Commensurate with the Executive Order, we are circulating a draft PDD to address the overall security oversight structure which will parallel the reform you directed in the counterintelligence area.

RECOMMENDATIONS

That you approve a judicially reviewable public interest balancing test for the declassification of records.

Approve _____ Disapprove _____

That you approve automatic declassification of records at 25 years.

Approve _____ Disapprove _____

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

July 7, 1994

94 JUL 7 P7:19

MEMORANDUM FOR JOHN PODESTA
MORT HALPERIN
JAMES BAKER
STEVE GARFINKEL

THROUGH:

GEORGE TENET

FROM:

REGINA GENTON

SUBJECT:

Attorney General Views on the draft Executive Order on National Security Information

Attached for your information is a memorandum from the Attorney General to Tony Lake concerning Department of Justice opposition to certain provisions in the draft Executive Order on the classification and declassification of National Security Information. As you know, the principal unresolved issue is the advisability of a "back-end" public interest balancing test which may be the subject of a future White House staff meeting. We are continuing to work with the FBI to address its implementation of the automatic declassification provision, and I believe we can accept DoJ's suggested revision of the "reasonable doubt" provision (change "reasonable" doubt to "significant" or "substantial" doubt).

Attachment

Tab I Memorandum from the Attorney General



Office of the Attorney General
Washington, D. C. 20530

June 30, 1994

MEMORANDUM FOR: THE ASSISTANT TO THE PRESIDENT
FOR NATIONAL SECURITY AFFAIRS
THE COUNSEL TO THE PRESIDENT

FROM: THE ATTORNEY GENERAL *[Signature]*

SUBJECT: Proposed Executive Order on National Security Information

The Deputy Attorney General's April 20, 1994 Memorandum for the Assistant to the President for National Security Affairs (attached at Tab A) set forth three problems created by the draft Executive Order on classified national security information: (1) the substantial logistical problems that the automatic declassification provisions pose for the FBI; (2) the litigation risks created by the balancing provisions; and (3) the litigation risks posed by the "reasonable doubt" provisions. That Memorandum also proposed specific alternatives to these provisions that would ameliorate these problems.

On May 24, a group of DoJ and FBI representatives met with representatives of the NSC to discuss these problems and the proposed solutions. Since that meeting, the FBI has informally proposed several options that would mitigate the logistical problems posed by the declassification provisions. It is my understanding, however, that this issue remains unresolved.

The other two problems also have not been resolved. If left in their current form, the public interest balancing test and reasonable doubt provisions would make it more difficult for the Department of Justice to defend Executive Branch classification decisions. These provisions would invite courts to substitute their judgment for that of the Executive in matters affecting national security. Accordingly, we continue to believe that these provisions should be deleted from the draft order or, in the alternative, revised in the manner discussed in the Deputy Attorney General's April 20 Memorandum and in this Memorandum.

I understand the sentiment that the increased judicial scrutiny that would be occasioned by these provisions is desirable, because it would discourage excessive classification and encourage declassification, thereby promoting openness in government. But the Administration's new FOIA policy, set forth in statements by the President and by me last October, and its government-wide access initiatives do a great deal to promote

openness in government. Executive agencies should be given the chance to make this commitment to openness work before their classification and declassification decisions are subjected to additional review by courts.

More importantly, the draft order already provides administrative procedures to check significant over-classification, including: (1) the Interagency Security Classification Appeals panel, which will review appeals of decisions denying requests for mandatory declassification; (2) the Information Security Oversight Office, which is empowered to conduct on-site reviews of agencies' classification programs; (3) the requirement that agencies establish and maintain self-inspection programs to review and assess their classified product; and (4) the requirement that each agency's Inspector General also conduct periodic evaluations of the agency's classification program. In light of these procedures, heightened judicial scrutiny of Executive Branch decisions in this area should be unnecessary and, as discussed below, may well have undesirable results.

I. THE PUBLIC INTEREST BALANCING TEST

A. The Draft Order

As currently drafted, section 3.2(b) of the draft Executive Order provides:

If an agency head or senior agency official determines that the public interest in disclosure of specific information classified by that agency outweighs the national security interest in its continued classification, the information shall be declassified even though it continues to meet the standards for classification under this Order.¹

As discussed in the Deputy Attorney General's April 20 Memorandum, this provision could undermine the Department's ability successfully to defend Executive Branch classification decisions. Although courts traditionally have deferred to the Executive's judgment concerning whether disclosure of information would damage national security, it is our fear that courts could decide that the Executive Branch has no special expertise in assessing the "public interest" in disclosure, and therefore might accord an agency's application of the balancing test little deference. The addition of this "public interest" factor, then,

¹ Section 1.2(b) of the draft order provides for a similar balancing test at the initial classification stage. The NSC has informed us, however, that section 1.2(b) will be deleted from the order.

may invite courts to substitute their judgment for Executive Branch judgments. This result would be inconsistent with the Executive's constitutional responsibility to protect national security information.

Moreover, even if courts in the end upheld the Executive's decisions, the addition of the balancing test provision is predicted to encourage litigation challenging particular applications of that provision, requiring depositions, detailed affidavits, production of deliberative documents, and possibly trials. This new litigation could pose a significant burden on both the Department and on the affected client agencies. We therefore continue to believe that the public interest balancing test should be deleted from the draft Executive Order.

B. The Carter Administration Order

It has been suggested that reinstating the balancing test provision of the Carter Administration's Executive Order (E.O. 12065) in lieu of the draft order's provision might ameliorate some of these problems. The balancing provision of the Carter order (section 3-303) was substantially similar to section 3.2(b) of the draft order. It provided:

It is presumed that information which continues to meet the classification requirements in Section 1-3 requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head, a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order, an official with Top Secret classification authority, or the Archivist of the United States in the case of material covered in Section 3-503. That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

(Emphases added.)

This provision was arguably slightly more protective of the Executive's prerogative in protecting national security information than the draft order. For example, the statement that properly classified information is "presumed" to require continued protection and the limitation of balancing to "some cases" permitted the Department to argue that balancing was not mandatory in all cases, but only in exceptional cases in which the relevant agency official determined, in his or her discretion, that balancing was appropriate.

Significantly, though, the Carter Administration concluded that this provision, standing alone, was insufficiently protective of governmental interests. For that reason, a Memorandum was issued by then-National Security Adviser Zbigniew Brzezinski stressing the discretionary nature of the balancing test. That Memorandum (attached at Tab B) emphasized that the balancing test did not apply to all declassification decisions, but only in "exceptional" and "rare" cases. It also specifically stated that the provision was "not intended to modify the substantive criteria or procedures for classification," but simply "reflect[ed] th[e] Administration's policy that properly classified information nevertheless may be declassified under some circumstances." Finally, the Brzezinski Memorandum made clear that the balancing test was a "discretionary determination[.]" See, e.g., Salisbury v. United States, 690 F.2d 966 (D.C. Cir. 1982) (relying in part on Brzezinski Memorandum in holding that balancing test was discretionary).

Even with the Brzezinski Memorandum, however, the Carter order's language prompted litigation over a host of issues, including: (1) whether balancing of the public interest was mandatory or discretionary; (2) whether an agency's failure to balance or its assessment of the national security/public interest balance was subject to judicial review; (3) if judicial review was available, whether the agency's decision should be accorded deference or reviewed de novo; and (4) whether the "public interest" had to be considered at the initial classification stage as well as the declassification stage.²

Circumstances with regard to FOIA litigation have changed dramatically since the Carter Administration. There is far more litigation under FOIA in general today, and the FOIA requester community and bar are more specialized and sophisticated than they were in the late 1970s and early 1980s. As a result, reinstating the Carter order's balancing test would engender considerably more litigation today than E.O. 12065 did during the

² See e.g., McGehee v. Casey, No. 81-0734 (D.D.C. Sept. 25, 1981), 718 F.2d 1137 (D.C. Cir. 1983); Afshar v. Dept. of State, 76-1421 (D.D.C. Oct. 24, 1980), aff'd in part, vac'd in part, rev'd in part and remanded, 702 F.2d 1125 (D.C. Cir. 1983); Halkin v. Helms (Halkin II), 690 F.2d 977 (D.C. Cir. 1982); Salisbury v. United States, No. 80-909 (D.D.C. April 14, 1981), aff'd, 690 F.2d 966 (D.C. Cir. 1982); Allen v. CIA, 636 F.2d 1287 (D.C. Cir. 1980), on remand, 516 F. Supp. 653 (D.D.C. 1981); Andres v. CIA, No. 80-0865 (D.D.C. April 28, 1981), rev'd and remanded, 673 F.2d 550 (D.C. Cir. 1981) (table) (unpublished); Marks v. Casey, No. 77-1108 (D.D.C. July 28, 1981); Patterson v. CIA, No. 78-0070 (D.D.C. Feb. 5, 1981); Ground Saucer Watch, Inc. v. CIA, No. 78-859 (D.D.C. May 10, 1980); Kanter v. Dept. of State, 479 F. Supp. 921 (D.D.C. 1979).

Carter Administration.

C. Options

1. No Public Interest Balancing Test. For the reasons set forth above and in the Deputy Attorney General's April 20 Memorandum, the Department of Justice continues to recommend that the public interest balancing test be deleted from the draft order. Any balancing test, even if accompanied by language emphasizing the discretionary nature of the test, will increase the amount of litigation challenging declassification decisions. Moreover, inclusion of a balancing test could undermine judicial deference to the Executive's determinations in this area.

2. Carter "Plus." As noted in the April 20 Memorandum, if some form of balancing test is desired, there should be an explicit statement that balancing is an exercise of Executive Branch discretion and does not create any rights subject to judicial review, just as the Brzezinski Memorandum made it explicit that the balancing test under the Carter order was discretionary. The Administration's position would be consistent with, but clearer than, the Carter order and would represent how the Carter order was, in fact, implemented. The Carter order could be revised as follows (with the revisions in boldface):

It is presumed that information that continues to meet the classification requirements under this Order requires continued protection. In some **exceptional** cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order. That official will determine, **as an exercise of discretion**, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

This provision does not amplify or modify the substantive criteria or procedures for classification, and does not create any substantive or procedural rights subject to judicial review.³

³ My October 4, 1993 Memorandum for Heads of Departments and Agencies encouraging the use of "discretionary disclosures" under FOIA contained a similar disclaimer: "[T]his policy is not

II. REASONABLE DOUBT STANDARD

Sections 1.2(c) and 1.3(c) of the draft order provide that if there is "reasonable doubt" about the need to classify information or about the appropriate level of classification, the information shall not be classified or shall be classified at the lower level. These provisions create two significant problems. First, it is unclear how these provisions are intended to interact with the substantive criteria for classification. Information may be classified if disclosure "reasonably could be expected to cause damage" to the national security. Since "reasonably ... expected" clearly does not require a classifying authority to be certain that harm would result,⁴ the substantive criteria permit classification even where there is some uncertainty -- some doubt -- about the expected damage. Yet, the reasonable doubt provisions instruct classifying authorities not to classify information, or to classify at the lower level, if they have "reasonable doubt" about the need for classification or about the appropriate level of classification. At best, then, the reasonable doubt provisions would cause confusion. At worst, they would cause the release of information that is likely -- albeit not certain -- to harm national security.

Second, as stated in the April 20 Memorandum, the reasonable doubt provisions invite plaintiffs to argue that the government must prove "beyond a reasonable doubt" that its classification decisions are correct. If adopted by a court, this standard would impose an extremely high burden of proof on the government in defending its classification decisions. As noted above, we would prefer that the administrative procedures of the draft order serve as the mechanism for discouraging over-classification.

A. Options

1. No "Reasonable Doubt" Language. For the reasons discussed above, the reasonable doubt provisions should be deleted. The order instead could admonish agency officials to bear in mind the Administration's policy of avoiding unnecessary

intended to create any substantive or procedural rights enforceable at law."

⁴ Cf. Keys v. United States Dep't of Justice, 830 F.2d 337, 346 (D.C. Cir. 1987) (under FOIA exemption 7(C), which protects law enforcement information the disclosure of which "could reasonably be expected to constitute an unwarranted invasion of personal privacy," the "government need not 'prove to a certainty that release will lead to an unwarranted invasion of personal privacy'" (citation omitted), rev'd on other grounds, 489 U.S. 749 (1989).

classification. Section 1.2(c) could be revised as follows:

In applying the standards for classification, the original classification authority shall bear in mind the importance of avoiding unnecessary classification of information.

Similarly, section 1.3(c) could read:

In applying the standards for classification, the original classification authority shall bear in mind the importance of not classifying information at a higher level of classification than is warranted.

2. "Significant" or "Substantial" Doubt. If, despite the litigation risks, some "doubt" language is desired, we think at the very least that "reasonable doubt" should be replaced with "substantial doubt" or "significant doubt." These revisions would avoid the risk of subjecting the government to the extremely high "beyond a reasonable doubt" standard in justifying its classification decisions. We should emphasize, however, that these options would still pose substantial litigation risks and invite courts to second-guess Executive Branch determinations affecting national security. We therefore think that any provision utilizing "doubt" language should be accompanied by an explicit statement that the provision does not create any substantive or procedural rights subject to judicial review, such as:

This provision does not amplify or modify the substantive criteria or procedures for classification, and does not create any substantive or procedural rights subject to judicial review.

* * *

Please let me know if you would like to discuss these or any other proposed alternatives.



Office of the Deputy Attorney General

Washington, D.C. 20530

April 20, 1994

MEMORANDUM FOR THE ASSISTANT TO THE PRESIDENT
FOR NATIONAL SECURITY AFFAIRS

FROM: THE DEPUTY ATTORNEY GENERAL *JS9*
RE: Revision of Executive Order 12356 on
National Security Information

William Itoh's March 17, 1994 memorandum requests comments on a draft Executive Order to replace Executive Order 12356, "National Security Information." This draft attempts to establish a new security system that is committed both to greater openness in government and to the protection of truly sensitive information based on the principles of cost effectiveness and risk management.

As you know, in October 1993 the President and the Attorney General launched a major initiative on openness in government. As part of this initiative, the Attorney General has made a commitment to reduce the growing and complex problem of administrative backlogs in processing Freedom of Information/Privacy Act requests for access to records by the public. This Department's backlog, for example, has grown by 48% since 1987 and currently exceeds 37,000 requests. In evaluating the proposed Executive Order, I think it important to look not only at the policy objectives of the draft but also how the proposal would impact the already dramatic pledges the President and the Department have made to facilitating access to government records, reducing backlogs, and streamlining the administrative process.

In this regard and despite the laudable objectives of the order, it has substantial problems as presently drafted because it does not adequately protect truly sensitive information, is not cost effective, and will substantially contribute to the backlogs we are trying to reduce in order to achieve real openness in government. In addition, certain provisions of the order may impair this Department's ability to successfully defend the Executive's national security classification decisions against legal challenges.

* * * *

Automatic Declassification

The primary way in which the order seeks to declassify information and reduce the amount of classified information -- goals shared by this Department -- is by requiring automatic declassification of all twenty-five year old information within four years of the effective date of the order except that which is specifically exempted by the agency head. This requirement will necessitate a commitment of new resources that is simply not foreseeable or possible, significantly increase administrative backlogs of access requests, and place extremely sensitive information at risk of disclosure.

As a practical matter, massive resources either must be acquired or diverted from other Department responsibilities for a document-by-document review of all twenty-five year old information if sensitive information is to be protected from inadvertent automatic declassification under circumstances in which it can never be reclassified.

For example, the Federal Bureau of Investigation -- only one component of this Department with significant amounts of classified material -- (1) does not have a system for tracking existing documents by age or (2) identifying which files contain classified information. Even limiting the review to those files likely to contain the vast majority of classified information, there are in excess of (3) 100,000 such files that are over twenty-five years old. (4) The average file contains approximately 250 (5) pages, which means that the Bureau would have to review over one hundred million pages of classified documents during the initial four year period provided for in the order.

(6) Assuming that the review of this dated material will take one-fifth the time needed to review more recent information, (7) it would still require 270 new analysts at a cost exceeding (8) \$54,000,000, as well as an additional (9) sixty-five support personnel, to staff such a project. (10) Alternatively, some or all of the 155 analysts currently devoted to processing Freedom of Information Act (FOIA) requests and litigation discovery requests could be detailed to declassification review but only at the cost of either bringing the release of information under the FOIA and litigation discovery requests to a complete halt or adding significantly to the FOIA backlog the Attorney General has pledged to reduce as part of her openness in government initiative.

(11) The only other option is to assign Special Agents on a TDY basis to headquarters. The cost of this solution would exceed \$60,000,000 if we were to accept the consequences of diverting these agents from their primary law enforcement and counterintelligence duties. None of these alternatives is realistic or cost effective.

I am aware that some thought has been given to allowing a senior official to identify information by category for exemption from automatic declassification without prior review of the information involved. I have serious doubts that such an exercise can be undertaken with sufficient certainty that all sensitive information could be identified and exempted from disclosure.

The vast majority of FBI national security investigative records are not, by their nature, susceptible to categorization and exemption by file. Thus, in the absence of a specific review, the imprecision of such an exercise will necessarily result in either too much or too little information being declassified. Although both results are of concern to me, the former presents potentially grave consequences for the national security and the FBI's ability to fulfill its intelligence mission.

Moreover, even if our records could be categorized by file, no declassified file can be released without review for other applicable exemptions from mandatory release under the FOIA and/or the Privacy Act. A document-by-document review would be still be necessary to make the openness contemplated by the order a reality. Thus, the practical result of this provision is either that the declassified information will not be released as expected by the public, which is not openness in government, or that we have imposed upon ourselves the FOIA administrator's worst nightmare -- a request for access to all classified agency records over twenty-five years old.

There is a more straightforward and cost-effective way to reduce the amount of classified information. Automatic declassification should only focus on twenty-five year old records that the public has specifically requested. This information could then be processed for release under the order's stringent standards for twenty-five year old information, thus eliminating wasteful reviews of unrequested information while maintaining very strict standards for continuing classification beyond twenty-five years. Realistic systematic review, also called for in the draft order, could address the legitimate needs of historians.

The one disadvantage of this approach is that it does not eliminate, and perhaps invites, a request from a member of the public for all classified records in an agency over twenty-five years old. However, the only way to totally avoid this possibility is to not impose any date for automatic declassification, a option that may be unacceptable to the administration. Accordingly, we must be prepared to resist any such overbroad request in litigation.

*

*

*

*

Litigation Issues

Balancing Test. With respect to the Department of Justice's ability to successfully defend national security disclosure decisions, courts have in the past uniformly deferred to the Executive's judgment in recognition of the President's constitutional authority and responsibility to protect national security information. The addition of a public interest balancing test will encourage today's sophisticated FOIA litigants to argue that the Executive's determinations as to the public interest are judicially reviewable and, because the Executive has no particular expertise -- or at least not the exclusive responsibility -- on this issue, are entitled to no deference. Through the mechanism of reviewing the public interest decision, courts will be able to second-guess and overrule our national security judgments.

Given the broad spectrum of interest groups, it is not hard to imagine that almost all of the President's foreign policy decisions, including special activities, will be subject to a judicially reviewable public interest balancing in which it will be argued that the Executive's judgment is entitled to no deference. Factual issues are also likely to arise concerning the level and specificity of proof necessary to sustain the government's burden. Litigation of these issues may result in the probing of the basis for classification decisions through discovery (with depositions and requests for deliberative documents), and perhaps trial.

Inviting the judiciary to assume such a role would be improvident and could be viewed as inconsistent with the Executive's constitutional responsibility to protect national security information. Therefore, I believe that the "balancing test" should be deleted from the draft order. At a minimum, if it is desirable to retain some reference to the public interest in the order, the two provisions at issue should be revised to require only "consideration" of the public interest in disclosure. We would be happy to work with you on specific language.

In the alternative, and recognizing that the risks described above would only be reduced and not eliminated, section 1.2(b) should be deleted from the order, and section 3.2(b) revised to read:

Information that continues to meet the standards for classification under this order shall remain classified unless an agency head or senior agency official determines, as an exercise of discretion, that the public interest in disclosure of specific information classified by that agency outweighs the national security interest in its continued classification.

Another alternative that would reduce litigation risks, but not as much as the second option, would be to revise section 3.2(b) as described above and retain section 1.2(b) but amended to read:

Information that meets the standards for classification shall be classified unless the original classification authority determines, as an exercise of discretion, that the public interest in keeping the information unclassified outweighs the need for classification.

Judicial Review. Furthermore, in order to further insulate balancing decisions from review and to help ensure that the decisions of the Interagency Security Classification Appeals Panel on classification challenges and mandatory review requests are final and not subject to judicial review, a new provision should be added at the end of the order as follows:

This Executive order is not intended to, and does not, create any right to judicial review, or any other right, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, additional to those created by statute. Furthermore, all provisions referring to balancing the public interest are separate from the substantive and procedural criteria for classification and are not intended to amplify or modify those criteria in any respect.

Reasonable Doubt Standard. The final issue that may impair our ability to defend the classification of sensitive information in litigation involves sections 1.2(c) and 1.3(c). These sections require that, if there is reasonable doubt about the need to classify information or about the appropriate level of classification, it shall not be classified or shall be classified at the lower level. While I support the spirit and intent of these provisions, they will, as presently formulated, increase the risk of litigation by inviting a resourceful plaintiff to argue that the government must prove "beyond a reasonable doubt" that its classification decisions are correct. If adopted by a court -- a not unrealistic possibility -- a very high burden of proof, akin to that used in criminal prosecutions, would have to be met in order to successfully defend classification decisions in FOIA litigation. I do not believe that anyone intends such a result and suggest that these provisions be deleted or substantially redrafted.

*

*

*

*

General Suggestions

Finally, we have several general suggestions to improve the order. First, in order to avoid confusion and sanctions against employees acting in good faith, the word "negligently" should be deleted from sections 5.1(b) and 5.7(b) of the order. Mechanisms already exist for dealing with employees who make honest mistakes.

Second, although section 3.4(b) would most likely cover the potential circumstances when continued classification beyond twenty-five years is necessary, it would appear prudent to provide flexibility to take into account the unusual case where the national security may require continued classification and none of the categories apply. I, therefore, suggest adding the following at the end of this subsection:

Upon the recommendation of the Interagency Security Classification Appeals Panel, the Assistant to the President for National Security Affairs may exempt from automatic declassification specific information that does not fall within one of these categories.

* * * *

Department of Justice Point of Contact

Mr. Richard Scruggs, Acting Counsel for Intelligence Policy, (202)514-5600, is our point of contact on this issue and is available to discuss this matter with your staff.

THE WHITE HOUSE
WASHINGTON

#78065

November 30, 1978

Dear Dr. Rhoads:

This is in response to your letter of November 28, in which you request my views on the implementation of the balancing test in section 3-303 of Executive Order 12065.

The purpose of the balancing test provision is to permit the declassification of properly classified information in those exceptional cases where the public interest in protection of such information is outweighed by the public interest in its disclosure. The Order recognizes that cases meeting the criterion of section 3-303 will be rare, and that information considered for declassification that continues to meet the classification requirements of section 1-3 despite the passage of time must, in most cases, remain classified.

This provision is not intended to modify the substantive criteria or procedures for classification; rather, it reflects this Administration's policy that properly classified information nevertheless may be declassified under some circumstances. It is for these reasons that the provision was included in section 3-3 on declassification policy rather than in section 1, which details the relevant classification criteria.

The Order does not establish a particular procedure to be followed in those exceptional cases where section 3-303 might apply. Instead, it provides that when questions arise, a senior agency official will make the determination whether the public interest in disclosure outweighs the damage to the national security, and, hence, to the public interest, that might reasonably be expected to result from disclosure. Each agency should establish its own procedures to ensure that individuals making declassification decisions identify those cases that should be referred to senior agency officials designated to make the discretionary determinations under section 3-303.

Sincerely,



Zbigniew Brzezinski

Dr. James B. Rhoads
Interagency Classification Review Committee
Washington, D. C. 20408

LA 061

June 30, 1994

ACTION

MEMORANDUM FOR ANTHONY LAKE

THROUGH: GEORGE TENET
MORT HALPERIN

FROM: REGINA GENTON

SUBJECT: Draft Executive Order on National Security Information

We have concluded our review of agency comments on the draft Executive Order on the classification and declassification of national security information, and made a number of significant changes to address the major concerns of the principal agencies (State, Defense, CIA and Justice). There are several issues, however, where we have not fully accommodated agency views and where there may be a difference of opinion among the President's senior advisers.

First, you should know that we have largely accommodated agency concerns on the automatic declassification provision by:

- Extending the time to come into compliance from four years to five years.
- Allowing agencies to exempt certain "file series of records" where the information almost invariably falls within one of the exemption categories. This will mean, for example, that all CIA agent case files will be exempt.
- Making automatic declassification applicable only to records that have permanent historical value (instead of all "information"), thereby reducing the volume of documents subject to declassification review. This will help some agencies significantly. For example, it will eliminate an estimated 40 percent of the documents CIA must review.

The FBI remains concerned about automatic declassification of their material, given the state of their file system. We will work with FBI Director Freeh to come up with a mutually satisfactory solution to the FBI's unique problem. As you will recall, we added a provision to the Order clarifying the fact that nothing in the Order limits the protection afforded any information by other provisions of law, including exemptions to the Freedom of Information Act (other than for classification), the Privacy Act and the National Security Act of 1947. Thus, many of the FBI's documents would continue to be protected under other FOIA exemptions which protect law enforcement equities.

There are several provisions where some agencies sought modifications that we did not believe we could change without altering the Executive Order in a fundamental way. Namely, whether the Executive Order should "automatically declassify" documents at 25 years (as most agencies prefer) or at 30 years, whether documents which contained any information qualifying for additional protection beyond 25 years could be left classified in their entirety (this is the so-called "redaction" issue the DCI raised with you), and whether the Order should contain a judicially reviewable public interest balancing test when agencies declassify

documents. The draft Order, as circulated to agencies last month, contained such a balancing test. The Department of Justice favors making the "back-end" balancing test purely discretionary and thus nonjudicable. Justice has been talking to Lloyd Cutler, who is sympathetic to their views. We believe that judicial review of the balancing test and automatic declassification are the most dramatic and important reforms in the current Order. Finally, agencies estimate the cost of reviewing the huge backlog of documents that are 25 years old or older (conservatively estimated at over 1 billion pages), as required by the draft Order, would cost on the order of \$450 million over five years. (Attached at Tab I is a background paper which lays out these issues in more detail.)

The next step in finalizing a new Executive Order is OMB's formal coordination with Executive Branch agencies and release to the public for comment. **Before proceeding to this step, we believe it is prudent to resolve any substantive differences of view among the President's senior advisers and to seek a Presidential decision on key policy issues. Lloyd Cutler in particular recommends a meeting to discuss the balancing test and resource implications of the Order. We believe you should talk to Lloyd directly and then decide whether to convene a meeting of senior White House advisers to discuss these issues.**

Under separate cover, we have sent you a PDD to address problems in the government's oversight and policy structure with respect to security issues. Our goal is to release a new E.O. and a PDD at the same time, given the overlapping nature of the two issues.

Concurrences by: James Baker William Leary

RECOMMENDATION

That you read the background paper at Tab I on the major policy issues in the Executive Order and meet with us to discuss these matters.

Approve _____ Disapprove _____

That you speak with Lloyd Cutler regarding his concerns and convene a meeting of senior White House advisers to consider and resolve any differences of view regarding the Order before issues are put before the President for decision. In addition to you and Lloyd, we recommend John Podesta, George Stephanopoulos and Jack Quinn also be invited to participate in these discussions.

Approve _____ Disapprove _____

Attachments

Tab I	Background on Major Issues in the Executive Order
Tab II	Draft Executive Order

BACKGROUND ON THE MAJOR ISSUES IN THE EXECUTIVE ORDER ON NATIONAL SECURITY INFORMATION

I. PUBLIC INTEREST BALANCING TEST

At issue is whether the Executive Order should require agencies to balance the public interest in disclosure against the possible harm to national security in deciding whether to declassify information (known as the balancing test) and whether that decision should be subject to court review under the Freedom of Information Act (FOIA).

A word of explanation is required. The FOIA provides that information may be withheld if it is properly classified pursuant to an Executive Order. Persons seeking documents under the FOIA can challenge a decision to withhold in a lawsuit and the court makes a de novo interpretation as to whether the information fits within the exemption. Thus, whatever standard for declassification is written into the Executive Order becomes the standard for judicial review in an FOIA lawsuit.

The draft order, as it was circulated to the agencies, requires a balancing test both at the time of classification and when a declassification request is made. We are now planning to remove the requirement for balancing at the front end, but to leave in the requirement to balance when doing a declassification review and to make that judgment subject to the FOIA.

The only agency to raise objections to this is the Department of Justice, which defends all FOIA cases in court. Justice wants the balancing test removed or at a minimum made purely discretionary so we can argue it is not subject to judicial review. Its argument is that there will be an added burden of defending withholding information based on the argument that the public value of the information outweighs the harm to national security and that a court might order the disclosure of information that the government wanted to keep secret. In other words, the courts will look to the factual basis behind application of the test which will impose additional requirements on officials who prepare and sign declarations.

Our response is that the balancing test is one of the most important reforms in the Order and one of great value to the public interest community and the press. It reflects the President's commitment to openness and to the view that the public value of information should be taken into account in deciding whether to release information. Removing the balancing test, or rewriting it to preclude judicial review would be seen as an enormous step backward in disclosure policy. (The Carter Order had a balancing test, but the government proceeded to argue that it was discretionary and therefore not subject to judicial review. The courts agreed)

We agree with Justice that including a balancing test subject to judicial review will increase the burden of defending FOIA cases. However, we view this as a necessary and acceptable cost to force agencies to consider the public value of information before deciding whether to release information requested under the FOIA. The only effective way to impose that process on the bureaucracy is to make it a part of the Executive Order which is subject to judicial review. If judicial review is not available, agencies will not take the requirement seriously.

At the same time, we think there is no real danger that information would be ordered released by the courts which you or senior officials do not believe should be disclosed. Courts have been and will continue to be extraordinarily deferential to executive branch judgments about national security. In fact, no court has ever issued a final order directing the release of information which the government argued was properly classified. We think that judges would defer to the affidavit of a senior government official that, even taking account of the public value, the information should remain classified. A tentative decision by a District Court judge to order disclosure would always be subject to a motion to reconsider or to a stay pending appeal. Thus, there will always be an opportunity to provide a more persuasive affidavit from a more senior official or even to invoke Executive Privilege.

II. AUTOMATIC DECLASSIFICATION OF DOCUMENTS 25 YEARS OLD

The draft Executive Order would be the first to establish automatic declassification or a "drop dead" date for previously classified information. As a practical matter, unless we go to a system which does away with line-by-line and document-by-document review, we will never be able to address effectively the hundreds of millions of pages of classified material awaiting review. The draft Order, as it has been circulated to the agencies, would require that any records over 25 years old be automatically declassified. A document could be exempted from automatic declassification at the end of 25 years only by the head of the agency and only if the information fell into one of seven very narrow categories:

1. Reveal the identify of a confidential human source, or reveal information about the application of an intelligence source or method.
2. Reveal information that would assist in the development or use of weapons of mass destruction.
3. Reveal information that would impair US cryptologic systems or activities.
4. Reveal information that would impair the application of state of the art technology within a US weapon system.
5. Reveal actual US military war plans that remain in effect.
6. Reveal information that would cause exceptionally grave damage to the relations between the US and a foreign government.
7. Violate a statute, treaty, or international agreement.

It is our expectation that only a very small percentage of documents would require continued classification. However, nothing in the Order would limit the protection afforded by other laws, e.g., the Privacy Act, the National Security Act of 1947 and the Freedom of Information Act, so documents might continue to be withheld on grounds other than classification.

Most agencies favor a 30 year (instead of 25 year) "drop dead" date for the declassification of records for a number of reasons: it would reduce the immediate drain on agency resources for the review of older records; documents that are 30 years old will be slightly less sensitive than documents 25 years old; a 30 year standard would be consistent with both the Federal Records

Act which requires agencies to offer permanently valuable records to the National Archives when they become 30 years old, and with the State Department's Basic Authorities Act which requires the State Department to declassify certain records of historical value at 30 years.

Our response is that the Joint Security Commission (established by the DCI and Secretary of Defense last year to review our overall security system) recommended a 25 year "drop dead" date with similar exemption categories. In addition, the acting Archivist, in a letter to the Vice President pursuant to the National Performance Review, said that there are virtually no records over 25 years old that need to remain classified on national security grounds.

While all agencies now concede they do not oppose automatic declassification in principle, they will claim they do not have the resources to carry out the Order and thus the USG risks disclosing information damaging to the national security. While making the threshold for automatic declassification at 30 years instead of 25 years would make some difference in cost, that difference is at the margin and we do not believe cost should drive the decision on this matter.

We recommend you support automatic declassification at 25 years. Agencies do not have problems with the concept of automatic declassification; cost is their real concern. Increasing the automatic declassification time frame would be seen as a significant retreat in disclosure policy.

III. IMPLEMENTATION COSTS

The most costly element of the proposed Executive Order is declassifying the enormous backlog of documents that are 25 years old or older. The draft Executive Order gives agencies five years to clear the backlog. At the end of that period, documents would be declassified whether or not they had been reviewed. However, as noted above, some documents might still be withheld on other grounds or be subject to review for Privacy Act information before they could be made publicly available. No one knows the real size of the backlog, but it is conservatively estimated at over a billion pages. According to preliminary figures compiled by the DCI, it will cost the USG on the order of \$100 million per year for five years to address the backlog.

The DCI has argued that implementation costs could be reduced by one-third if agencies were permitted to keep entire documents classified if the document contained any information that qualified for continued protection beyond 25 years. We believe this would undermine fundamentally the principle of automatic declassification -- the centerpiece of the proposed Executive Order -- and subject the Order to severe criticism by public interest groups.

We want to stress that the cost estimates are soft. Agencies will have to develop a "risk management" methodology to review their documents, and may find it will cost less -- or more -- than these current rough estimates. While the cost is not trivial, when considered against what the government spends to maintain the current security system, estimated at \$16 billion annually, we believe it is worth dedicating the necessary funds now to address the backlog. No one has faced up to the problem in the past, and it will only become increasingly insurmountable as time passes. What is equally important is that we put in place a system prospectively in which documents are marked in such a way that declassification is truly automatic and done at minimal cost to the Government.

There undoubtedly will be a cost to the Government to declassify old records, but we believe the cost does not outweigh the benefit of public access to and confidence in the workings of its government.



Office of the Attorney General
Washington, D. C. 20530

June 30, 1994

MEMORANDUM FOR: THE ASSISTANT TO THE PRESIDENT
FOR NATIONAL SECURITY AFFAIRS
THE COUNSEL TO THE PRESIDENT

FROM: THE ATTORNEY GENERAL *[Signature]*

SUBJECT: Proposed Executive Order on National Security Information

The Deputy Attorney General's April 20, 1994 Memorandum for the Assistant to the President for National Security Affairs (attached at Tab A) set forth three problems created by the draft Executive Order on classified national security information: (1) the substantial logistical problems that the automatic declassification provisions pose for the FBI; (2) the litigation risks created by the balancing provisions; and (3) the litigation risks posed by the "reasonable doubt" provisions. That Memorandum also proposed specific alternatives to these provisions that would ameliorate these problems.

On May 24, a group of DoJ and FBI representatives met with representatives of the NSC to discuss these problems and the proposed solutions. Since that meeting, the FBI has informally proposed several options that would mitigate the logistical problems posed by the declassification provisions. It is my understanding, however, that this issue remains unresolved.

The other two problems also have not been resolved. If left in their current form, the public interest balancing test and reasonable doubt provisions would make it more difficult for the Department of Justice to defend Executive Branch classification decisions. These provisions would invite courts to substitute their judgment for that of the Executive in matters affecting national security. Accordingly, we continue to believe that these provisions should be deleted from the draft order or, in the alternative, revised in the manner discussed in the Deputy Attorney General's April 20 Memorandum and in this Memorandum.

I understand the sentiment that the increased judicial scrutiny that would be occasioned by these provisions is desirable, because it would discourage excessive classification and encourage declassification, thereby promoting openness in government. But the Administration's new FOIA policy, set forth in statements by the President and by me last October, and its government-wide access initiatives do a great deal to promote

openness in government. Executive agencies should be given the chance to make this commitment to openness work before their classification and declassification decisions are subjected to additional review by courts.

More importantly, the draft order already provides administrative procedures to check significant over-classification, including: (1) the Interagency Security Classification Appeals panel, which will review appeals of decisions denying requests for mandatory declassification; (2) the Information Security Oversight Office, which is empowered to conduct on-site reviews of agencies' classification programs; (3) the requirement that agencies establish and maintain self-inspection programs to review and assess their classified product; and (4) the requirement that each agency's Inspector General also conduct periodic evaluations of the agency's classification program. In light of these procedures, heightened judicial scrutiny of Executive Branch decisions in this area should be unnecessary and, as discussed below, may well have undesirable results.

I. THE PUBLIC INTEREST BALANCING TEST

A. The Draft Order

As currently drafted, section 3.2(b) of the draft Executive Order provides:

If an agency head or senior agency official determines that the public interest in disclosure of specific information classified by that agency outweighs the national security interest in its continued classification, the information shall be declassified even though it continues to meet the standards for classification under this Order.¹

As discussed in the Deputy Attorney General's April 20 Memorandum, this provision could undermine the Department's ability successfully to defend Executive Branch classification decisions. Although courts traditionally have deferred to the Executive's judgment concerning whether disclosure of information would damage national security, it is our fear that courts could decide that the Executive Branch has no special expertise in assessing the "public interest" in disclosure, and therefore might accord an agency's application of the balancing test little deference. The addition of this "public interest" factor, then,

¹ Section 1.2(b) of the draft order provides for a similar balancing test at the initial classification stage. The NSC has informed us, however, that section 1.2(b) will be deleted from the order.

may invite courts to substitute their judgment for Executive Branch judgments. This result would be inconsistent with the Executive's constitutional responsibility to protect national security information.

Moreover, even if courts in the end upheld the Executive's decisions, the addition of the balancing test provision is predicted to encourage litigation challenging particular applications of that provision, requiring depositions, detailed affidavits, production of deliberative documents, and possibly trials. This new litigation could pose a significant burden on both the Department and on the affected client agencies. We therefore continue to believe that the public interest balancing test should be deleted from the draft Executive Order.

B. The Carter Administration Order

It has been suggested that reinstating the balancing test provision of the Carter Administration's Executive Order (E.O. 12065) in lieu of the draft order's provision might ameliorate some of these problems. The balancing provision of the Carter order (section 3-303) was substantially similar to section 3.2(b) of the draft order. It provided:

It is presumed that information which continues to meet the classification requirements in Section 1-3 requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head, a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order, an official with Top Secret classification authority, or the Archivist of the United States in the case of material covered in Section 3-503. That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

(Emphases added.)

This provision was arguably slightly more protective of the Executive's prerogative in protecting national security information than the draft order. For example, the statement that properly classified information is "presumed" to require continued protection and the limitation of balancing to "some cases" permitted the Department to argue that balancing was not mandatory in all cases, but only in exceptional cases in which the relevant agency official determined, in his or her discretion, that balancing was appropriate.

Significantly, though, the Carter Administration concluded that this provision, standing alone, was insufficiently protective of governmental interests. For that reason, a Memorandum was issued by then-National Security Adviser Zbigniew Brzezinski stressing the discretionary nature of the balancing test. That Memorandum (attached at Tab B) emphasized that the balancing test did not apply to all declassification decisions, but only in "exceptional" and "rare" cases. It also specifically stated that the provision was "not intended to modify the substantive criteria or procedures for classification," but simply "reflect[ed] th[e] Administration's policy that properly classified information nevertheless may be declassified under some circumstances." Finally, the Brzezinski Memorandum made clear that the balancing test was a "discretionary determination[]." See, e.g., Salisbury v. United States, 690 F.2d 966 (D.C. Cir. 1982) (relying in part on Brzezinski Memorandum in holding that balancing test was discretionary).

Even with the Brzezinski Memorandum, however, the Carter order's language prompted litigation over a host of issues, including: (1) whether balancing of the public interest was mandatory or discretionary; (2) whether an agency's failure to balance or its assessment of the national security/public interest balance was subject to judicial review; (3) if judicial review was available, whether the agency's decision should be accorded deference or reviewed de novo; and (4) whether the "public interest" had to be considered at the initial classification stage as well as the declassification stage.²

Circumstances with regard to FOIA litigation have changed dramatically since the Carter Administration. There is far more litigation under FOIA in general today, and the FOIA requester community and bar are more specialized and sophisticated than they were in the late 1970s and early 1980s. As a result, reinstating the Carter order's balancing test would engender considerably more litigation today than E.O. 12065 did during the

² See e.g., McGehee v. Casey, No. 81-0734 (D.D.C. Sept. 25, 1981), 718 F.2d 1137 (D.C. Cir. 1983); Afshar v. Dept. of State, 76-1421 (D.D.C. Oct. 24, 1980), aff'd in part, vac'd in part, rev'd in part and remanded, 702 F.2d 1125 (D.C. Cir. 1983); Halkin v. Helms (Halkin II), 690 F.2d 977 (D.C. Cir. 1982); Salisbury v. United States, No. 80-909 (D.D.C. April 14, 1981), aff'd, 690 F.2d 966 (D.C. Cir. 1982); Allen v. CIA, 636 F.2d 1287 (D.C. Cir. 1980), on remand, 516 F. Supp. 653 (D.D.C. 1981); Andres v. CIA, No. 80-0865 (D.D.C. April 28, 1981), rev'd and remanded, 673 F.2d 550 (D.C. Cir. 1981) (table) (unpublished); Marks v. Casey, No. 77-1108 (D.D.C. July 28, 1981); Patterson v. CIA, No. 78-0070 (D.D.C. Feb. 5, 1981); Ground Saucer Watch, Inc. v. CIA, No. 78-859 (D.D.C. May 10, 1980); Kanter v. Dept. of State, 479 F. Supp. 921 (D.D.C. 1979).

Carter Administration.

C. Options

1. No Public Interest Balancing Test. For the reasons set forth above and in the Deputy Attorney General's April 20 Memorandum, the Department of Justice continues to recommend that the public interest balancing test be deleted from the draft order. Any balancing test, even if accompanied by language emphasizing the discretionary nature of the test, will increase the amount of litigation challenging declassification decisions. Moreover, inclusion of a balancing test could undermine judicial deference to the Executive's determinations in this area.

2. Carter "Plus." As noted in the April 20 Memorandum, if some form of balancing test is desired, there should be an explicit statement that balancing is an exercise of Executive Branch discretion and does not create any rights subject to judicial review, just as the Brzezinski Memorandum made it explicit that the balancing test under the Carter order was discretionary. The Administration's position would be consistent with, but clearer than, the Carter order and would represent how the Carter order was, in fact, implemented. The Carter order could be revised as follows (with the revisions in boldface):

It is presumed that information that continues to meet the classification requirements under this Order requires continued protection. In some **exceptional** cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order. That official will determine, **as an exercise of discretion**, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

This provision does not amplify or modify the substantive criteria or procedures for classification, and does not create any substantive or procedural rights subject to judicial review.³

³ My October 4, 1993 Memorandum for Heads of Departments and Agencies encouraging the use of "discretionary disclosures" under FOIA contained a similar disclaimer: "[T]his policy is not

II. REASONABLE DOUBT STANDARD

Sections 1.2(c) and 1.3(c) of the draft order provide that if there is "reasonable doubt" about the need to classify information or about the appropriate level of classification, the information shall not be classified or shall be classified at the lower level. These provisions create two significant problems. First, it is unclear how these provisions are intended to interact with the substantive criteria for classification. Information may be classified if disclosure "reasonably could be expected to cause damage" to the national security. Since "reasonably ... expected" clearly does not require a classifying authority to be certain that harm would result,⁴ the substantive criteria permit classification even where there is some uncertainty -- some doubt -- about the expected damage. Yet, the reasonable doubt provisions instruct classifying authorities not to classify information, or to classify at the lower level, if they have "reasonable doubt" about the need for classification or about the appropriate level of classification. At best, then, the reasonable doubt provisions would cause confusion. At worst, they would cause the release of information that is likely -- albeit not certain -- to harm national security.

Second, as stated in the April 20 Memorandum, the reasonable doubt provisions invite plaintiffs to argue that the government must prove "beyond a reasonable doubt" that its classification decisions are correct. If adopted by a court, this standard would impose an extremely high burden of proof on the government in defending its classification decisions. As noted above, we would prefer that the administrative procedures of the draft order serve as the mechanism for discouraging over-classification.

A. Options

1. No "Reasonable Doubt" Language. For the reasons discussed above, the reasonable doubt provisions should be deleted. The order instead could admonish agency officials to bear in mind the Administration's policy of avoiding unnecessary

intended to create any substantive or procedural rights enforceable at law."

⁴ Cf. Keys v. United States Dep't of Justice, 830 F.2d 337, 346 (D.C. Cir. 1987) (under FOIA exemption 7(C), which protects law enforcement information the disclosure of which "could reasonably be expected to constitute an unwarranted invasion of personal privacy," the "government need not 'prove to a certainty that release will lead to an unwarranted invasion of personal privacy'" (citation omitted), rev'd on other grounds, 489 U.S. 749 (1989).

classification. Section 1.2(c) could be revised as follows:

In applying the standards for classification, the original classification authority shall bear in mind the importance of avoiding unnecessary classification of information.

Similarly, section 1.3(c) could read:

In applying the standards for classification, the original classification authority shall bear in mind the importance of not classifying information at a higher level of classification than is warranted.

2. "Significant" or "Substantial" Doubt. If, despite the litigation risks, some "doubt" language is desired, we think at the very least that "reasonable doubt" should be replaced with "substantial doubt" or "significant doubt." These revisions would avoid the risk of subjecting the government to the extremely high "beyond a reasonable doubt" standard in justifying its classification decisions. We should emphasize, however, that these options would still pose substantial litigation risks and invite courts to second-guess Executive Branch determinations affecting national security. We therefore think that any provision utilizing "doubt" language should be accompanied by an explicit statement that the provision does not create any substantive or procedural rights subject to judicial review, such as:

This provision does not amplify or modify the substantive criteria or procedures for classification, and does not create any substantive or procedural rights subject to judicial review.

* * *

Please let me know if you would like to discuss these or any other proposed alternatives.

T
A
B
A



Office of the Deputy Attorney General

Washington, D.C. 20530

April 20, 1994

MEMORANDUM FOR THE ASSISTANT TO THE PRESIDENT
FOR NATIONAL SECURITY AFFAIRS

FROM:

THE DEPUTY ATTORNEY GENERAL *JS9*

RE:

Revision of Executive Order 12356 on
National Security Information

William Itoh's March 17, 1994 memorandum requests comments on a draft Executive Order to replace Executive Order 12356, "National Security Information." This draft attempts to establish a new security system that is committed both to greater openness in government and to the protection of truly sensitive information based on the principles of cost effectiveness and risk management.

As you know, in October 1993 the President and the Attorney General launched a major initiative on openness in government. As part of this initiative, the Attorney General has made a commitment to reduce the growing and complex problem of administrative backlogs in processing Freedom of Information/Privacy Act requests for access to records by the public. This Department's backlog, for example, has grown by 48% since 1987 and currently exceeds 37,000 requests. In evaluating the proposed Executive Order, I think it important to look not only at the policy objectives of the draft but also how the proposal would impact the already dramatic pledges the President and the Department have made to facilitating access to government records, reducing backlogs, and streamlining the administrative process.

In this regard and despite the laudable objectives of the order, it has substantial problems as presently drafted because it does not adequately protect truly sensitive information, is not cost effective, and will substantially contribute to the backlogs we are trying to reduce in order to achieve real openness in government. In addition, certain provisions of the order may impair this Department's ability to successfully defend the Executive's national security classification decisions against legal challenges.

*

*

*

*

Automatic Declassification

The primary way in which the order seeks to declassify information and reduce the amount of classified information -- goals shared by this Department -- is by requiring automatic declassification of all twenty-five year old information within four years of the effective date of the order except that which is specifically exempted by the agency head. This requirement will necessitate a commitment of new resources that is simply not foreseeable or possible, significantly increase administrative backlogs of access requests, and place extremely sensitive information at risk of disclosure.

As a practical matter, massive resources either must be acquired or diverted from other Department responsibilities for a document-by-document review of all twenty-five year old information if sensitive information is to be protected from inadvertent automatic declassification under circumstances in which it can never be reclassified.

For example, the Federal Bureau of Investigation -- only one component of this Department with significant amounts of classified material -- (1) does not have a system for tracking existing documents by age or (2) identifying which files contain classified information. Even limiting the review to those files likely to contain the vast majority of classified information, there are in excess of (3) 100,000 such files that are over twenty-five years old. (4) The average file contains approximately 250 (5) pages, which means that the Bureau would have to review over one hundred million pages of classified documents during the initial four year period provided for in the order.

(6) Assuming that the review of this dated material will take one-fifth the time needed to review more recent information, (7) it would still require 270 new analysts at a cost exceeding (8) \$54,000,000, as well as an additional (9) sixty-five support personnel, to staff such a project. (10) Alternatively, some or all of the 155 analysts currently devoted to processing Freedom of Information Act (FOIA) requests and litigation discovery requests could be detailed to declassification review but only at the cost of either bringing the release of information under the FOIA and litigation discovery requests to a complete halt or adding significantly to the FOIA backlog the Attorney General has pledged to reduce as part of her openness in government initiative.

The only other option is to assign (11) Special Agents on a TDY basis to headquarters. The cost of this solution would exceed \$60,000,000 if we were to accept the consequences of diverting these agents from their primary law enforcement and counterintelligence duties. None of these alternatives is realistic or cost effective.

I am aware that some thought has been given to allowing a senior official to identify information by category for exemption from automatic declassification without prior review of the information involved. I have serious doubts that such an exercise can be undertaken with sufficient certainty that all sensitive information could be identified and exempted from disclosure.

The vast majority of FBI national security investigative records are not, by their nature, susceptible to categorization and exemption by file. Thus, in the absence of a specific review, the imprecision of such an exercise will necessarily result in either too much or too little information being declassified. Although both results are of concern to me, the former presents potentially grave consequences for the national security and the FBI's ability to fulfill its intelligence mission.

Moreover, even if our records could be categorized by file, no declassified file can be released without review for other applicable exemptions from mandatory release under the FOIA and/or the Privacy Act. A document-by-document review would be still be necessary to make the openness contemplated by the order a reality. Thus, the practical result of this provision is either that the declassified information will not be released as expected by the public, which is not openness in government, or that we have imposed upon ourselves the FOIA administrator's worst nightmare -- a request for access to all classified agency records over twenty-five years old.

There is a more straightforward and cost-effective way to reduce the amount of classified information. Automatic declassification should only focus on twenty-five year old records that the public has specifically requested. This information could then be processed for release under the order's stringent standards for twenty-five year old information, thus eliminating wasteful reviews of unrequested information while maintaining very strict standards for continuing classification beyond twenty-five years. Realistic systematic review, also called for in the draft order, could address the legitimate needs of historians.

The one disadvantage of this approach is that it does not eliminate, and perhaps invites, a request from a member of the public for all classified records in an agency over twenty-five years old. However, the only way to totally avoid this possibility is to not impose any date for automatic declassification, a option that may be unacceptable to the administration. Accordingly, we must be prepared to resist any such overbroad request in litigation.

*

*

*

*

Litigation Issues

Balancing Test. With respect to the Department of Justice's ability to successfully defend national security disclosure decisions, courts have in the past uniformly deferred to the Executive's judgment in recognition of the President's constitutional authority and responsibility to protect national security information. The addition of a public interest balancing test will encourage today's sophisticated FOIA litigants to argue that the Executive's determinations as to the public interest are judicially reviewable and, because the Executive has no particular expertise -- or at least not the exclusive responsibility -- on this issue, are entitled to no deference. Through the mechanism of reviewing the public interest decision, courts will be able to second-guess and overrule our national security judgments.

Given the broad spectrum of interest groups, it is not hard to imagine that almost all of the President's foreign policy decisions, including special activities, will be subject to a judicially reviewable public interest balancing in which it will be argued that the Executive's judgment is entitled to no deference. Factual issues are also likely to arise concerning the level and specificity of proof necessary to sustain the government's burden. Litigation of these issues may result in the probing of the basis for classification decisions through discovery (with depositions and requests for deliberative documents), and perhaps trial.

Inviting the judiciary to assume such a role would be improvident and could be viewed as inconsistent with the Executive's constitutional responsibility to protect national security information. Therefore, I believe that the "balancing test" should be deleted from the draft order. At a minimum, if it is desirable to retain some reference to the public interest in the order, the two provisions at issue should be revised to require only "consideration" of the public interest in disclosure. We would be happy to work with you on specific language.

In the alternative, and recognizing that the risks described above would only be reduced and not eliminated, section 1.2(b) should be deleted from the order, and section 3.2(b) revised to read:

Information that continues to meet the standards for classification under this order shall remain classified unless an agency head or senior agency official determines, as an exercise of discretion, that the public interest in disclosure of specific information classified by that agency outweighs the national security interest in its continued classification.

Another alternative that would reduce litigation risks, but not as much as the second option, would be to revise section 3.2(b) as described above and retain section 1.2(b) but amended to read:

Information that meets the standards for classification shall be classified unless the original classification authority determines, as an exercise of discretion, that the public interest in keeping the information unclassified outweighs the need for classification.

Judicial Review. Furthermore, in order to further insulate balancing decisions from review and to help ensure that the decisions of the Interagency Security Classification Appeals Panel on classification challenges and mandatory review requests are final and not subject to judicial review, a new provision should be added at the end of the order as follows:

This Executive order is not intended to, and does not, create any right to judicial review, or any other right, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, additional to those created by statute. Furthermore, all provisions referring to balancing the public interest are separate from the substantive and procedural criteria for classification and are not intended to amplify or modify those criteria in any respect.

Reasonable Doubt Standard. The final issue that may impair our ability to defend the classification of sensitive information in litigation involves sections 1.2(c) and 1.3(c). These sections require that, if there is reasonable doubt about the need to classify information or about the appropriate level of classification, it shall not be classified or shall be classified at the lower level. While I support the spirit and intent of these provisions, they will, as presently formulated, increase the risk of litigation by inviting a resourceful plaintiff to argue that the government must prove "beyond a reasonable doubt" that its classification decisions are correct. If adopted by a court -- a not unrealistic possibility -- a very high burden of proof, akin to that used in criminal prosecutions, would have to be met in order to successfully defend classification decisions in FOIA litigation. I do not believe that anyone intends such a result and suggest that these provisions be deleted or substantially redrafted.

General Suggestions

Finally, we have several general suggestions to improve the order. First, in order to avoid confusion and sanctions against employees acting in good faith, the word "negligently" should be deleted from sections 5.1(b) and 5.7(b) of the order. Mechanisms already exist for dealing with employees who make honest mistakes.

Second, although section 3.4(b) would most likely cover the potential circumstances when continued classification beyond twenty-five years is necessary, it would appear prudent to provide flexibility to take into account the unusual case where the national security may require continued classification and none of the categories apply. I, therefore, suggest adding the following at the end of this subsection:

Upon the recommendation of the Interagency Security Classification Appeals Panel, the Assistant to the President for National Security Affairs may exempt from automatic declassification specific information that does not fall within one of these categories.

* * * *

Department of Justice Point of Contact

Mr. Richard Scruggs, Acting Counsel for Intelligence Policy, (202)514-5600, is our point of contact on this issue and is available to discuss this matter with your staff.

THE WHITE HOUSE

WASHINGTON

#78065

November 30, 1978

Dear Dr. Rhoads:

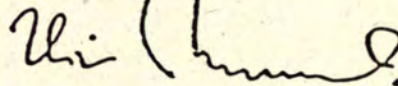
This is in response to your letter of November 28, in which you request my views on the implementation of the balancing test in section 3-303 of Executive Order 12065.

The purpose of the balancing test provision is to permit the declassification of properly classified information in those exceptional cases where the public interest in protection of such information is outweighed by the public interest in its disclosure. The Order recognizes that cases meeting the criterion of section 3-303 will be rare, and that information considered for declassification that continues to meet the classification requirements of section 1-3 despite the passage of time must, in most cases, remain classified.

This provision is not intended to modify the substantive criteria or procedures for classification; rather, it reflects this Administration's policy that properly classified information nevertheless may be declassified under some circumstances. It is for these reasons that the provision was included in section 3-3 on declassification policy rather than in section 1, which details the relevant classification criteria.

The Order does not establish a particular procedure to be followed in those exceptional cases where section 3-303 might apply. Instead, it provides that when questions arise, a senior agency official will make the determination whether the public interest in disclosure outweighs the damage to the national security, and, hence, to the public interest, that might reasonably be expected to result from disclosure. Each agency should establish its own procedures to ensure that individuals making declassification decisions identify those cases that should be referred to senior agency officials designated to make the discretionary determinations under section 3-303.

Sincerely,



Zbigniew Brzezinski

Dr. James B. Rhoads
Interagency Classification Review Committee
Washington, D. C. 20408

LA 061



Washington, D.C. 20520

June 23, 1994

MEMORANDUM FOR WILLIAM H. ITOH
EXECUTIVE SECRETARY
NATIONAL SECURITY COUNCIL

SUBJECT: Nomination for Commission on Protecting and Reducing
Government Secrecy

The Foreign Relations Authorization Act for Fiscal Years 1994 and 1995, signed into law on April 30, established a Commission on Protecting and Reducing Government Secrecy. The Commission is to be composed of twelve members, including two appointed by the President from the Executive Branch of Government. The Department of State strongly believes that the Assistant Secretary for Diplomatic Security, currently Anthony C.E. Quainton, should be one of the appointees.

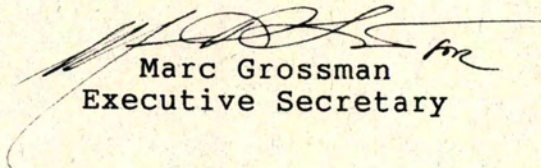
The Assistant Secretary for Diplomatic Security is the Department's senior agency official having primary responsibility to oversee its Information Security Program, including policies relating to classification, declassification, protection of classified information, and employee information security awareness education. The Bureau of Diplomatic Security (DS) also conducts the Department's personnel security clearance investigations to certify eligibility for access to classified information.

As a "laboratory" in the National Performance Review ("Reinventing Government"), DS has been a leader in working to streamline the background investigations process -- one of the Commission's mandates. Common investigative standards among agencies have been adopted, and common adjudicative standards are being developed. DS is exploring with all other foreign affairs agencies the consolidation of security functions, including background investigations.

During the past year, the Department has put in place an effective program for the identification, declassification review, and transfer to the National Archives of its 30-year-old and older records for public review. Through its demonstration that large quantities of previously classified records can be made accessible to the public quickly and relatively economically, this program has become a model for other agencies.

The Commission will be entirely funded by the Department, which will also provide facilities, staff and other support services. For these reasons, we strongly believe that the Department should be represented on the Commission and that the appropriate representative is the Assistant Secretary for Diplomatic Security.

Thank you for your assistance.



Marc Grossman
Executive Secretary

Feb 21
2-5
208 EOB

John:

Attached is a compilation of all the comments to the EO compiled by Steve Garfinkel

Next Tuesday, February 21, from 2-5pm in Room 208 we will sit down to review the comments and make final decisions on what to take etc. Meeting will include, Gina, myself, Mark Halperin, Garfinkel.

It would be terrific and productive if you could set the time aside and attend.

Cheers.

Greg Tackett

AGENCY COMMENTS

DRAFT EXECUTIVE ORDER
ON
CLASSIFIED NATIONAL SECURITY
INFORMATION

AS COLLATED & SYNOPSIZED
BY THE
INFORMATION SECURITY
OVERSIGHT OFFICE

February 10, 1995

TABLE OF CONTENTS

Preamble	1
----------------	---

Part 1. Original Classification

1.1	Definitions	2
1.2	Classification Standards	5
1.3	Classification Levels	6
1.4	Classification Authority	7
1.5	Classification Categories	9
1.6	Duration of Classification	10
1.7	Identification and Markings	12
1.8	Classification Prohibitions and Limitations	15
1.9	Classification Challenges	16

Part 2. Derivative Classification

2.1	Definitions	17
2.2	Use of Derivative Classification	19
2.3	Classification Guides	19

Part 3. Declassification and Downgrading

3.1	Definitions	20
3.2	Authority for Declassification	22
3.3	Transferred Information	24
3.4	Automatic Declassification	25
3.5	Systematic Declassification Review	29
3.6	Mandatory Declassification Review	30
3.7	Processing Requests and Reviews	33
3.8	Declassification Database	34

Part 4. Safeguarding

4.1	Definitions	34
4.2	General Restrictions on Access	36
4.3	Distribution Controls	38
4.4	Special Access Programs	39
4.5	Access by Historical Researchers and Former Presidential Appointees	41

Part 5. Implementation and Review

5.1	Definitions	42
5.2	Policy Direction	43
5.3	Information Security Oversight Office	43
5.4	Interagency Security Classification Appeals Panel ..	45
5.5	Information Security Policy Advisory Council	47
5.6	General Responsibilities	49
5.7	Sanctions	51

Part 6. General Provisions

6.1	General Provisions	53
6.2	Effective Date	54

Executive Order
Classified National Security Information

This Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information.

Our democratic principles require that the American people be informed concerning the activities of their Government. Also, our nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations.

Protecting information critical to our nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

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

Part 1

Original Classification

Section 1.1 *Definitions.*

As used in this Order, these terms are defined as follows:

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

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this Order or any predecessor order to require protection against disclosure.

(d) "Foreign Government Information" means:

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

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

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" has the meaning provided at 5 U.S.C. § 552(f).

(j) "Senior agency official" means the official designated by the agency head under Section 5.6(a)(3) of this Order to direct and administer the agency's program under which information is classified, safeguarded and declassified.

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

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the disclosure of information, to include the sensitivity, value, and utility of that information.

Section 1.2 *Classification Standards*

(a) Information may be originally classified under the terms of this Order only if all of the following conditions are met:

- (1) An original classification authority classifies the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in Section 1.5 of this Order; and
- (4) the original classification authority determines that the disclosure of the information reasonably could be expected to result in damage to the national security and the original classifier is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

- (1) Amplify or modify the substantive criteria or procedures for classification; and
- (2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Section 1.3 *Classification Levels.*

(a) Information may be classified at one of the following three levels:

(1) **Top Secret** shall be applied to information, the disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) **Secret** shall be applied to information, the disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) **Confidential** shall be applied to information, the disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

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

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Section 1.4 *Classification Authority.*

(a) The authority to classify information originally may be exercised only by:

(1) The President;

(2) agency heads and officials designated by the President in the *Federal Register*; or

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) *Delegation of Original Classification Authority.*

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

(2) **Top Secret** original classification authority may be delegated only by the President; or an agency head or official designated pursuant to paragraph (a)(2), above.

(3) **Secret** or **Confidential** original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated **Top Secret** original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this Order and its implementing directives.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days

whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Section 1.5 *Classification Categories.*

Information may not be considered for classification unless it concerns:

- (a) Military plans, weapons, or operations;
- (b) Foreign government information;
- (c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- (d) Foreign relations or foreign activities of the United States, including confidential sources;
- (e) Scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

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

Section 1.6 *Duration of Classification.*

(a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for automatic declassification ten years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for a period not to exceed ten additional years if such action is consistent with the standards and

procedures established under this Order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from automatic declassification specific information the disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

- (1) Reveal an intelligence source, method, or activity, or a cryptologic system or activity;

- (2) reveal information that would assist in the development or use of weapons of mass destruction;

- (3) reveal information that would impair the development or use of technology within a United States weapon system;

- (4) reveal United States military plans, or national security emergency preparedness plans;

- (5) reveal foreign government information;

- (6) damage relations between the United States and a foreign government, or reveal a confidential source;

(7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or

(8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with Part 3 of this Order.

Section 1.7 *Identification and Markings.*

(a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) One of the three classification levels defined in Section 1.3 of this Order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) The date or event for declassification, as prescribed in Section 1.6(a) or Section 1.6(c);

(B) the date that is ten years from the date of original classification, as prescribed in Section 1.6(b); or

(C) the exemption category from automatic declassification, as prescribed in Section 1.6(d); and

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in Section 1.5 of this Order.

(b) Specific information contained in paragraph (a), above, shall be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from automatic declassification under Section 1.6(d) of this Order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this Order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Marking designations implementing the provisions of this Order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued by the Director of the Information Security Oversight Office.

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

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Section 1.8 *Classification Prohibitions and Limitations.*

(a) In no case shall information be classified in order to:

- (1) Conceal violations of law, inefficiency, or administrative error;
- (2) prevent embarrassment to a person, organization, or agency;
- (3) restrain competition; or
- (4) prevent or delay the release of information that does not require

protection in the interest of national security.

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

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act of 1974 (5 U.S.C. § 552a), or the mandatory review provisions of Section 3.6 of this Order only if such classification meets the requirements of this Order and is accomplished on a document-by-document basis under the personal participation or direction of the agency head, the

deputy agency head, or the senior agency official designated under Section 5.6 of this Order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44 United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

- (1) Meets the standards for classification under this Order; and
- (2) is not otherwise revealed in the individual items of information.

As used in this Order, "compilation" means an arrangement of pre-existing unclassified items of information gathered together.

Section 1.9 *Classification Challenges.*

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued by the Director of the Information Security Oversight Office, an agency head or senior agency official shall establish procedures under which authorized holders of information shall challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

- (1) individuals are not subject to retribution for bringing such actions;
- (2) an opportunity is provided for review by an impartial official or panel;
- and (3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by Section 5.4 of this Order.

Part 2

Derivative Classification

Section 2.1 *Definitions.*

As used in this Order, these terms are defined as follows:

(a) "Derivative classification" means the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification

includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document which contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides or a combination of both.

Section 2.2 *Use of Derivative Classification.*

(a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

- (1) Observe and respect original classification decisions; and
- (2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward: (A) the date or event for declassification that corresponds to the longest period of classification among the sources; and (B) a listing of these sources on or attached to the official file or record copy.

Section 2.3 *Classification Guides.*

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this Order.

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

(1) Has program or supervisory responsibility over the information or is the senior agency official; and

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

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this Order.

Part 3

Declassification and Downgrading

Section 3.1 Definitions.

As used in this Order, these terms are defined as follows:

(a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

(1) The occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this Order.

(c) "Declassification authority" means:

(1) The official who authorized the original classification, if that official is still serving in the same position;

(2) the originator's successor;

(3) a supervisory official of either; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of this Order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Section 3.2 *Authority for Declassification.*

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this Order.

(b) It is presumed that information that continues to meet the classification requirements under this Order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in

these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or a senior agency official with responsibility for processing Freedom of Information Act requests or mandatory review requests under this Order. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

- (1) Amplify or modify the substantive criteria or procedures for classification; and
- (2) create any substantive or procedural rights subject to judicial review.

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

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

Section 3.3 *Transferred Information.*

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

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

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

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives.

However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in Sections 1.6 and 3.4 of this Order.

Section 3.4 *Automatic Declassification.*

(a) Subject to paragraph (b), below, within five years from the issuance of this Order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

- (1) Reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method;
- (2) reveal information that would assist in the development or use of weapons of mass destruction;
- (3) reveal information that would impair United States cryptologic systems or activities;
- (4) reveal information that would impair the application of state of the art technology within a United States weapon system;
- (5) reveal actual United States military war plans that remain in effect;
- (6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government; or
- (7) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this Order, an agency head shall notify the President through the National Security Council of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) A description of the file series;
- (2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before it becomes subject to automatic declassification under this Section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as executive secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) A description of the information;
- (2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date

than recommended. The agency head may appeal such a decision to the President through the National Security Council. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this Order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan of action for compliance with the requirements of this Section, including the establishment of interim target dates. Each such plan of action shall include the requirement that the agency declassify at least 15 percent of the records affected by this Section no later than one year from the effective date of this Order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this Section shall remain subject to the mandatory and systematic declassification review provisions of this Order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this Section for a period longer than 25 years from the date of their creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this Section.

Section 3.5 *Systematic Declassification Review.*

(a) Each agency that has originated classified information under this Order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records excepted from automatic declassification under Section 3.4 of this Order. Agencies shall prioritize the systematic review of records based upon:

(1) Recommendations of the Information Security Policy Advisory Council, established in Section 5.5 of this Order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist of the United States shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives of the United States as of the effective date of this Order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall prioritize the systematic review of these records based upon the recommendations of the Information Security Policy Advisory

Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this Order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

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

Section 3.6 *Mandatory Declassification Review.*

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

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

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and

(3) the information has not been reviewed for declassification within the past two years. If the agency has reviewed the information within the past two years, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

(4) others specifically providing advice and counsel to the incumbent President or acting on behalf of the incumbent President

is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code.

Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Agencies with primary subject

matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this Order. They shall release this information unless withholding is otherwise authorized and necessary under applicable law.

(d) In accordance with directives issued pursuant to this Order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

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

Section 3.7 *Processing Requests and Reviews.*

In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order, or pursuant to the automatic declassification or systematic review provisions of this Order:

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

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this Order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this Order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Section 3.8 *Declassification Database.*

(a) The Archivist of the United States, in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Government-wide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise provided by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

Part 4

Safeguarding

Section 4.1 *Definitions.*

As used in this Order, these terms are defined as follows:

- (a) "Safeguarding" means measures and controls that are prescribed to protect classified information.
- (b) "Access" means the ability or opportunity to gain knowledge of classified information.
- (c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform a lawful and authorized function.
- (d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.
- (e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.
- (f) "Network" means a system of two or more computers which can exchange data or information.
- (g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Section 4.2 *General Restrictions on Access.*

(a) A person may have access to classified information provided that:

- (1) A determination of trustworthiness has been made by an agency head or the agency head's designee;
- (2) the person has signed an approved nondisclosure agreement; and
- (3) the person has a need-to-know the information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Authorized dissemination of classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, which collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

- (1) Prevent access by unauthorized persons; and
- (2) ensure the integrity of the information.

(f) Consistent with law, directives and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this Order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less

restrictive than the safeguarding standards that ordinarily apply to United States **Confidential** information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this Section, the Department of Defense shall be considered one agency.

Section 4.3 *Distribution Controls.*

(a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Section 4.4 *Special Access Programs.*

(a) *Establishment of special access programs.* Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

- (1) The vulnerability of, or threat to, specific information is exceptional; and
- (2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or
- (3) the program is required by statute.

(b) *Requirements and limitations.*

(1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing extra protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives promulgated by the Director of the Information Security Oversight Office.

(3) Special access programs shall be subject to the oversight program established under Section 5.6(a)(3) of this Order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this Order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy and the Executive Secretary of the National Security Council or designee shall review annually each special access program to determine whether it continues to meet the requirements of this Order.

(c) Within 180 days after the effective date of this Order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this Order. Each existing special access program that an agency head or principal deputy revalidates shall be treated as if it were established on the effective date of this Order.

(d) Nothing in this Order shall supersede any requirement made by or under 10 U.S.C. § 119.

Section 4.5 *Access by Historical Researchers and Former Presidential Appointees.*

(a) The requirement in Section 4.2(a)(3) of this Order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

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

(b) Waivers under this Section may be granted only if the agency head or senior agency official of the originating agency:

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

Part 5

Implementation and Review

Section 5.1 *Definitions.*

(a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this Order and its implementing directives.

(b) "Violation" means:

(1) Any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful or negligent action to classify or continue the classification of information contrary to the requirements of this Order or its implementing directives; or

(3) any knowing, willful or negligent action to create or continue a special access program contrary to the requirements of this Order.

(c) "Infraction" means any knowing, willful or negligent action contrary to the requirements of this Order or its implementing directives that does not comprise a "violation," as defined above.

Section 5.2 *Policy Direction.*

(a) The National Security Council shall provide overall policy guidance for the program established under this Order.

(b) The Director of the Information Security Oversight Office shall be responsible for implementing and monitoring the program established under this Order.

Section 5.3 *Information Security Oversight Office.*

(a) There is established an Information Security Oversight Office.

(1) Remainder Reserved.

(b) The Director shall:

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

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

(3) review agency implementing regulations and agency guides for systematic declassification review. The Director shall require any regulation or guide to be changed if inconsistent with this Order or its implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guide shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of each agency's program established under this Order, and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the National Security Council within 60 days of the Director's request for access. Access shall be denied pending a prompt decision by the National Security Council;

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

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

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this Order;

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

(9) have the authority to convene and chair interagency or other meetings to discuss matters pertaining to the program established under this Order.

(c) Directives issued by the Director of the Information Security Oversight Office shall establish uniform standards for:

- (1) Safeguarding classified information;
- (2) agency security education and training programs;
- (3) agency self-inspection programs; and
- (4) classification and declassification guides.

Section 5.4 *Interagency Security Classification Appeals Panel.*

(a) *Establishment and Administration.*

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Executive Secretary of the National Security Council shall each appoint a senior level representative to serve as a member of the Panel. The President shall designate the Chairman of the Panel.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chairman. The Chairman shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) *Functions.* The Panel shall:

(1) Decide on appeals by persons who have filed classification challenges under Section 1.9 of this Order;

(2) approve, deny or amend agency exemptions from automatic declassification as provided in Section 3.4 of this Order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under Section 3.6 of this Order.

(c) *Rules and Procedures.* The Panel shall issue by-laws, which shall be published in the *Federal Register* no later than 120 days from the effective date of this Order. The by-laws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that:

(1) The Panel will consider appeals only on actions in which the appellant has exhausted his or her administrative remedies within the responsible agency, and there is no current action pending on the issue within the federal courts and the information has not been the subject of review by the federal courts or the Panel within the past two years;

(2) the Panel will assure compliance with the safeguarding requirements established by this Order and its implementing directives; and

(3) the Panel will report to the President through the National Security Council any instance in which it believes that an agency head is not cooperating fully with the Panel.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the National Security Council.

Section 5.5 *Information Security Policy Advisory Council.*

(a) *Establishment.* There is established an Information Security Policy Advisory Council ("Council"). The Council shall be comprised of seven members appointed by the President, from among interested persons who are

not otherwise employees of the Federal Government. The members shall elect the Council Chairman. The Council's by-laws shall establish standards for length of member service and rotation of the chair.

(b) *Functions.* The Council shall:

(1) Advise the President, the National Security Adviser, the Director of the Information Security Oversight Office, or such other executive branch officials as it deems appropriate, on policies established under this Order or its implementing directives, including recommended changes to those policies;

(2) recommend to agency heads specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) The Council shall meet at least twice each calendar year, and as otherwise provided in its by-laws.

(d) *Administration.*

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) The staff of the Information Security Oversight Office shall provide operational and administrative support for the Council.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, except that of reporting to the Congress, which are applicable to the Council, shall be performed in accordance with the guidelines and procedures established by the General Services Administration.

Section 5.6 *General Responsibilities.*

(a) Heads of agencies that originate or handle classified information shall:

(1) Demonstrate personal commitment and commit senior management to the successful implementation of the program established under this Order;

(2) commit necessary resources to the effective implementation of the program established under this Order;

(3) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(A) Overseeing the agency's program established under this Order, provided, an agency head may designate a separate official to oversee special access programs authorized under this Order. This official shall provide a full accounting of the agency's special access programs at least annually;

(B) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;

(C) establishing and maintaining security education and training programs;

(D) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

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

(F) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(G) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) Original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information; and

(H) accounting for the costs associated with the implementation of this Order, which shall be reported to the Director of the Information Security Oversight Office for publication.

(b) The Inspector General of each agency shall conduct periodic evaluations of the implementation and administration of the program established under this Order. To the extent permitted by statute, those portions of each Inspector General's reports that deal with this program shall be provided to the agency head and the Director of the Information Security Oversight Office.

Section 5.7 *Sanctions.*

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

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

(1) Disclose to unauthorized persons information properly classified under this Order or predecessor orders;

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

(3) create or continue a special access program contrary to the requirements of this Order; or

(4) contravene any other provision of this Order or its implementing directives.

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

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this Order.

(e) The agency head or senior agency official shall:

(1) Take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

Part 6

General Provisions

Section 6.1 *General Provisions.*

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

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

(c) Nothing in this Order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this Order.

Section 6.2 *Effective Date.*

This Order shall become effective 180 days from the date of its issuance.