

# Ronald Reagan Presidential Library Digital Library Collections

---

This is a PDF of a folder from our textual collections.

---

**Collection:** Roberts, John G.: Files  
**Folder Title:** JGR/Document Security  
**Box:** 17

---

To see more digitized collections visit:

<https://reaganlibrary.gov/archives/digital-library>

To see all Ronald Reagan Presidential Library inventories visit:

<https://reaganlibrary.gov/document-collection>

Contact a reference archivist at: [reagan.library@nara.gov](mailto:reagan.library@nara.gov)

Citation Guidelines: <https://reaganlibrary.gov/citing>

National Archives Catalogue: <https://catalog.archives.gov/>

THE WHITE HOUSE

WASHINGTON

February 10, 1983

MEMORANDUM FOR FRED F. FIELDING

FROM: JOHN G. ROBERTS *JGR*

SUBJECT: Document Security Memorandum

You asked that I rewrite, for style and order, the draft memorandum from John Rogers to the White House Staff on document security. I have attached a proposed draft.

Attachment

THE WHITE HOUSE

WASHINGTON

February 11, 1983

MEMORANDUM FOR WHITE HOUSE STAFF

FROM: FRED F. FIELDING  
COUNSEL TO THE PRESIDENT

SUBJECT: Document Security

Executive Order 12356, dated April 2, 1982, establishes rules for the classification, declassification, and safeguarding of information, the unauthorized disclosure of which could adversely affect national security. The purpose of this memorandum is to advise and remind you of security regulations concerning the safeguarding of classified information, and to assist you in meeting your individual security responsibilities.

There are three categories of classified national security information. The classifications are shown in descending order of sensitivity as they appear on classified documents:

Top Secret

Secret

Confidential

Access to classified information is permitted only if the recipient satisfies a two-part test. The recipient must (1) have the requisite security clearances, and (2) have a "need to know" the information to fulfill official Government duties or contractual obligations. In each instance, those possessing classified information must establish that the recipient has the requisite clearances and need to know. If in doubt, ask.

All employees who in any way receive classified information -- whether authorized or not -- have the responsibility to guard the information against disclosure to any unauthorized person. Anyone with knowledge of the loss, temporary loss of control or possession, or other possible compromise of classified information or material must immediately report the circumstances. Before termination of employment, an employee must transfer all classified material to a proper custodian with the necessary security clearances.

Never discuss classified information over a non-secure telephone or at non-official functions. Classified material may not be duplicated except in accordance with security

regulations; Top Secret material may not be reproduced without the permission of the originating agency.

All classified information must be stored in a safe having a three-position combination lock. Never leave such material unattended, and never place it in a desk drawer or other insecure place, even "temporarily." Lock safes when they are not in use and double check all safes at the end of the day to make sure they are locked. Commit safe combinations to memory, and restrict their knowledge to those who actually need to open and close the safes. Any problems encountered in opening or securing a safe should be reported immediately.

Many offices and agencies have developed procedures for identifying and labelling information which is sensitive, even though it may not be classified as top secret, secret, or confidential because it may not reasonably be expected to affect national security. Categorizations such as "limited official use" or "administratively sensitive" are typical examples. Employees who encounter such material should familiarize themselves with office rules concerning its dissemination, reproduction, and storage. These categorizations frequently identify material which is in some manner privileged information and/or is not to be disseminated beyond the particular office without appropriate approvals.

Any questions concerning the matters discussed in this memorandum should be directed to the Counsel's Office.

*John Roberts -  
Pls rewrite (style & over)*

THE WHITE HOUSE  
WASHINGTON

*do you wish to have  
this so you can  
signatures - who you  
suggested the instruction*

MEMORANDUM FOR:

~~WHITE HOUSE STAFF~~  
~~THE STAFF~~

FROM:

~~JOHN F. W. ROGERS~~  
~~DEPUTY ASSISTANT TO THE PRESIDENT~~  
~~FOR MANAGEMENT~~

SUBJECT:

~~Document Security~~  
~~PHYSICAL SECURITY INDOCTRINATION~~

*whether  
authorities  
or not*

*need of*  
Executive Order 12356 dated August 8, 1982 (revised) is concerned with classifying, declassifying, and safeguarding sensitive information, the unauthorized disclosure of which could adversely affect the national security. This memorandum ~~furnishes~~ *is to advise* information concerning security regulations based on the Order, and is designed to assist you in meeting your individual security responsibilities.

Only persons whose official duties require knowledge or possession of classified information are permitted to have access to this material. *For those who have clearance - if in doubt, check we same request does*

All employees who in any way receive classified information have the responsibility: (1) to guard it against disclosure to any unauthorized person; (2) not to duplicate it or permit its duplication by anyone except in accordance with security regulations; (3) to transfer before termination of employment all classified material to a proper custodian who possesses the necessary security clearance.

*↕*  
The loss or temporary loss of control or possession of classified information or material must be reported immediately.

There are three categories of classified national security data. These categories are shown in descending order of sensitivity as they will appear on classified documents:

Top Secret

Secret

Confidential

Access to classified information may be given only to an individual on a "need to know" basis. *and only if recipient has requested clearance* Never discuss classified or sensitive information over the telephone or at nonofficial functions.

Do not reproduce Top Secret information without the permission of the originating agency.

All classified information will be stored in a safe having a three-position combination lock. Never leave such material unattended, and never place it in a desk drawer or other insecure

places, even "temporarily". Lock safes when they are not in use and double check all safes at the end of the day to make sure they are locked. Commit safe combinations to memory, and restrict their knowledge to those who actually need to open and close the safes. Any problems encountered in opening or securing a safe should be reported immediately.

As an employee, you may become aware of information which is highly sensitive, although not classifiable from the standpoint of national defense. Information of this type is highly privileged, and must be treated as such. Never divulge such information to unauthorized persons, and be sure it is secure from unauthorized access while your office is unattended. ~~As a minimum, such material will be stored in a key locking cabinet. Storage in a safe is authorized.~~

Anyone having questions concerning this matter contact ~~George Saunders~~ on extension 2601.

Council's Office

(This is the category which we in the C.O. call "administrative capital" — think how to deal w/ that — see prior memos)

THE WHITE HOUSE

WASHINGTON

February 15, 1983

MEMORANDUM FOR WHITE HOUSE STAFF

FROM: FRED F. FIELDING *Orig. signed by FFE*  
COUNSEL TO THE PRESIDENT

SUBJECT: Document Security

Executive Order 12356, dated April 2, 1982, establishes rules for the classification, declassification, and safeguarding of information, the unauthorized disclosure of which could adversely affect national security. The purpose of this memorandum is to advise and remind you of security regulations concerning the safeguarding of classified information, and to assist you in meeting your individual security responsibilities.

There are three categories of classified national security information. The classifications are shown in descending order of sensitivity as they appear on classified documents:

Top Secret

Secret

Confidential

Access to classified information is permitted only if the recipient satisfies a two-part test. The recipient must (1) have the requisite security clearances, and (2) have a "need to know" the information to fulfill official Government duties or contractual obligations. In each instance, those possessing classified information must establish that the recipient has the requisite clearances and need to know. If in doubt, ask.

All employees who in any way receive classified information -- whether authorized or not -- have the responsibility to guard the information against disclosure to any unauthorized person. Anyone with knowledge of the loss, temporary loss of control or possession, or other possible compromise of classified information or material must immediately report the circumstances. Before termination of employment, an employee must transfer all classified material to a proper custodian with the necessary security clearances.

Never discuss classified information over a non-secure telephone or at non-official functions. Classified material may not be duplicated except in accordance with security



regulations; Top Secret material may not be reproduced without the permission of the originating agency.

All classified information must be stored in a safe having a three-position combination lock. Never leave such material unattended, and never place it in a desk drawer or other insecure place, even "temporarily." Lock safes when they are not in use and double check all safes at the end of the day to make sure they are locked. Commit safe combinations to memory, and restrict their knowledge to those who actually need to open and close the safes. Any problems encountered in opening or securing a safe should be reported immediately.

Many offices and agencies have developed procedures for identifying and labelling information which is sensitive, even though it may not be classified as top secret, secret, or confidential because it may not reasonably be expected to affect national security. Categorizations such as "administratively sensitive" are typical examples. Employees who encounter such material should familiarize themselves with office rules concerning its dissemination, reproduction, and storage. These categorizations frequently identify material which is in some manner privileged information and/or is not to be disseminated beyond the particular office without appropriate approvals.

Any questions concerning the matters discussed in this memorandum should be directed to the Counsel's Office.

FFF:JGR:aw 2/15/83

cc: FFFielding  
✓JGRoberts  
Subj.  
Chron




THE WHITE HOUSE

WASHINGTON

February 15, 1983

MEMORANDUM FOR WHITE HOUSE STAFF

FROM: FRED F. FIELDING   
COUNSEL TO THE PRESIDENT

SUBJECT: Document Security

Executive Order 12356, dated April 2, 1982, establishes rules for the classification, declassification, and safeguarding of information, the unauthorized disclosure of which could adversely affect national security. The purpose of this memorandum is to advise and remind you of security regulations concerning the safeguarding of classified information, and to assist you in meeting your individual security responsibilities.

There are three categories of classified national security information. The classifications are shown in descending order of sensitivity as they appear on classified documents:

Top Secret

Secret

Confidential

Access to classified information is permitted only if the recipient satisfies a two-part test. The recipient must (1) have the requisite security clearances, and (2) have a "need to know" the information to fulfill official Government duties or contractual obligations. In each instance, those possessing classified information must establish that the recipient has the requisite clearances and need to know. If in doubt, ask.

All employees who in any way receive classified information -- whether authorized or not -- have the responsibility to guard the information against disclosure to any unauthorized person. Anyone with knowledge of the loss, temporary loss of control or possession, or other possible compromise of classified information or material must immediately report the circumstances. Before termination of employment, an employee must transfer all classified material to a proper custodian with the necessary security clearances.

Never discuss classified information over a non-secure telephone or at non-official functions. Classified material may not be duplicated except in accordance with security

regulations; Top Secret material may not be reproduced without the permission of the originating agency.

All classified information must be stored in a safe having a three-position combination lock. Never leave such material unattended, and never place it in a desk drawer or other insecure place, even "temporarily." Lock safes when they are not in use and double check all safes at the end of the day to make sure they are locked. Commit safe combinations to memory, and restrict their knowledge to those who actually need to open and close the safes. Any problems encountered in opening or securing a safe should be reported immediately.

Many offices and agencies have developed procedures for identifying and labelling information which is sensitive, even though it may not be classified as top secret, secret, or confidential because it may not reasonably be expected to affect national security. Categorizations such as "administratively sensitive" are typical examples. Employees who encounter such material should familiarize themselves with office rules concerning its dissemination, reproduction, and storage. These categorizations frequently identify material which is in some manner privileged information and/or is not to be disseminated beyond the particular office without appropriate approvals.

Any questions concerning the matters discussed in this memorandum should be directed to the Counsel's Office.

*John Roberts  
pls rewrite (style over)*

THE WHITE HOUSE  
WASHINGTON

*fr. George Saunders*

*do you wish to have  
this go out over your  
signature - John Rogers  
suggested he check w/you*

MEMORANDUM FOR:

~~WHITE HOUSE STAFF~~  
~~THE STAFF~~

FROM:

~~JOHN F. W. ROGERS~~  
~~DEPUTY ASSISTANT TO THE PRESIDENT~~  
~~FOR MANAGEMENT~~

SUBJECT:

~~Document Security~~  
~~PHYSICAL SECURITY/INDOCTRINATION~~

*whether  
authorized  
or not*

*and send  
me 2*  
Executive Order 12356 dated August 8, 1982 (revised) is concerned with classifying, declassifying, and safeguarding sensitive information, the unauthorized disclosure of which could adversely affect the national security. This memorandum ~~furnishes~~ *is to advise* information concerning security regulations based on the Order, and is designed to assist you in meeting your individual security responsibilities.

Only persons whose official duties require knowledge or possession of classified information are permitted to have access to this material. *For those who have clearance - if in doubt, check we sure require docs*

All employees who in any way receive classified information have the responsibility: (1) to guard it against disclosure to any unauthorized person; (2) not to duplicate it or permit its duplication by anyone except in accordance with security regulations; (3) to transfer before termination of employment all classified material to a proper custodian who possesses the necessary security clearance.

The loss or temporary loss of control or possession of classified information or material must be reported immediately.

There are three categories of classified national security data. These categories are shown in descending order of sensitivity as they will appear on classified documents:

Top Secret

Secret

Confidential

Access to classified information may be given only to an individual on a "need to know" basis. *and only if request has clearance* Never discuss classified or sensitive information over the telephone or at nonofficial functions.

Do not reproduce Top Secret information without the permission of the originating agency.

All classified information will be stored in a safe having a three-position combination lock. Never leave such material unattended, and never place it in a desk drawer or other insecure

places, even "temporarily". Lock safes when they are not in use and double check all safes at the end of the day to make sure they are locked. Commit safe combinations to memory, and restrict their knowledge to those who actually need to open and close the safes. Any problems encountered in opening or securing a safe should be reported immediately.

As an employee, you may become aware of information which is highly sensitive, although not classifiable from the standpoint of national defense. Information of this type is highly privileged, and must be treated as such. Never divulge such information to unauthorized persons, and be sure it is secure from unauthorized access while your office is unattended. ~~As a minimum, such material will be stored in a key locking cabinet. Storage in a safe is authorized.~~

Anyone having questions concerning this matter contact ~~George Saunders~~ on extension 2601.

Council's Office

(This is the category which we in the C.D. call "adventurous capital" — think how to deal w/ that — see prior memos)

THE WHITE HOUSE

WASHINGTON

March 12, 1983

*file -  
classified information  
Doc. Security*

MEMORANDUM FOR ALL EXECUTIVE OFFICE OF THE PRESIDENT STAFF

FROM: JAMES A. BAKER III *JAB III*  
CHIEF OF STAFF AND  
ASSISTANT TO THE PRESIDENT

SUBJECT: Safeguarding National Security Information

The President has issued the attached National Security Decision Directive entitled "Safeguarding National Security Information," which is concerned with safeguarding against "unlawful disclosures of properly classified information." For the purposes of this Directive, the President has designated me as the "agency head" of the Executive Office of the President with responsibility for implementation of the Directive, including development and enforcement of appropriate policies consistent with its requirements.

Paragraphs 1 through 5 of the Directive require that internal procedures be developed both to safeguard against, and to govern the reporting and investigation of, unauthorized disclosures of classified information. I have directed the Counsel to the President to coordinate the development of such internal procedures for the Executive Office of the President, which shall include appropriate policies with respect to those limited instances in which polygraph testing may be appropriate.

Paragraph 1(d) of the Directive requires that appropriate policies be adopted to govern contacts between media representatives and agency personnel. On January 10, 1983, the attached "Guidelines for Press Coordination" were issued for the White House Staff, with instructions that all other elements of the Executive Office of the President "adopt parallel guidelines in coordination with the White House communications department." Compliance with these guidelines shall be the minimum action necessary to satisfy the Directive's requirements on contacts with media representatives.

Attachments

## Safeguarding National Security Information

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

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

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

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

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

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



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

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

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

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

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

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

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



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

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

5. The Office of Personnel Management and all departments and agencies with employees having access to classified information are directed to revise existing regulations and policies, as necessary, so that employees may be required to submit to polygraph examinations, when appropriate, in the course of investigations of unauthorized disclosures of classified information. As a minimum, such regulations shall permit an agency to decide that appropriate adverse consequences will follow an employee's refusal to cooperate with a polygraph examination that is limited in scope to the circumstances of the unauthorized disclosure under investigation. Agency regulations may provide that only the head of the agency, or his delegate, is empowered to order an employee to submit to a polygraph examination. Results of polygraph examinations should not be relied upon to the exclusion of other information obtained during investigations.

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

January 10, 1983

Guidelines for Press Coordination

1. The press office should remain the first stop for White House reporters seeking information about the President's policies and views.
2. In order to maintain an open Presidency, it is essential that members of the senior staff also be willing to meet with reporters on a frequent basis.
3. As the need arises, the communications department will designate key members of the staff who will be available to the press to answer questions on a specific subject. These "designated hitters" will be expected to take either telephone calls or be personally available to members of the press.
4. Requests for interviews or comments from members of the staff who have not been already designated to answer questions should first be referred to the communications department. After receiving a clearance or recommendation from the communications department, the staff member will be expected to make his or her own arrangements for the press interview. This procedure extends to the entire staff practices that are already followed in several departments of the White House.
5. Other departments that are part of the Executive Office of the President but are not formally part of the White House (e.g., NSC, OMB, CEA, Office of the Science Adviser) shall adopt parallel guidelines in coordination with the White House communications department.
6. The communications department will seek to ensure key members of the staff are sufficiently available to the press, especially on major news stories, to provide an open and full flow of information to the press.
7. As in the past, no member of the White House staff and related organizations shall accept a major television interview or large-scale press luncheon and breakfast without prior coordination with the communications department. In addition, it is recommended that all major interviews with groups of reporters inside the complex be held with a White House stenographer present.

8. On-the-record interviews should be recognized as the best way to conduct most interviews with the press.
9. The guidelines outlined here will apply whether the President is in Washington or out of town. They will not apply to strictly social engagements with members of the press.
10. In keeping with the traditions of this Presidency, these guidelines should be carried out in a way that maintains an atmosphere of openness, professionalism and civility in relations with the White House press corps.