BRIEF FOR PLAINTIFF-APPELLANT

IN THE

UNITED STATES COURT OF APPEALS

FOR THE DISTRICT OF COLUMBIA

No. 79-1700

HAROLD WEISBERG,

Plaintiff-Appellant

v.

CLARENCE M. KELLEY, ET AL.,

Defendants-Appellees

On Appeal from the United States District Court for the District of Columbia, Hon. John Lewis Smith, Jr., Judge

James H. Lesar
910 Sixteenth Street, N.W.
Washington, D.C. 20006

Attorney for Plaintiff-Appellant

BRIEF FOR PLAINTIFF-APPELLANT

IN THE

UNITED STATES COURT OF APPEALS

FOR THE DISTRICT OF COLUMBIA

No. 79-1700

HAROLD WEISBERG,

Plaintiff-Appellant

v.

CLARENCE M. KELLEY, ET AL.,

Defendants-Appellees

On Appeal from the United States District Court for the District of Columbia, Hon. John Lewis Smith, Jr., Judge

---

James H. Lesar
910 Sixteenth Street, N.W.
Washington, D.C. 20006

Attorney for Plaintiff-Appellant

IN THE

UNITED STATES COURT OF APPEALS

FOR THE DISTRICT OF COLUMBIA

HAROLD WEISBERG,	:	
	:	
Plaintiff-Appellant	:	
	:	
v.	:	Case No. 79-1700
	:	
	:	
CLARENCE M. KELLEY, ET AL.,	:	
	:	
Defendants-Appellees	:	

CERTIFICATE REQUIRED BY RULE 8(c) OF THE GENERAL RULES OF THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

Appellant certifies that the following listed parties and amici (if any) appeared below:

Harold Weisberg (Plaintiff)

Clarence M. Kelley (Defendant)

Griffin Bell (Defendant)

U.S. Department of Justice (Defendant)

These representations are made in order that judges of this Court, inter alia, may evaluate possible disqualification or recusal.

JAMES H. LESAR
Attorney for Appellant

TABLE OF CONTENTS

TABLE OF CASES

OTHER AUTHORITIES

*Cases chiefly relied upon are marked by asterisks

IN THE

UNITED STATES COURT OF APPEALS

FOR THE DISTRICT OF COLUMBIA

No. 79-1700

HAROLD WEISBERG,

Plaintiff-Appellant

v.

CLARENCE M. KELLEY, ET AL.,

Defendants-Appellees

On Appeal from the United States District Court for the District of Columbia, Hon. John Lewis Smith, Jr., Judge

---

BRIEF FOR PLAINTIFF-APPELLANT

STATEMENT OF ISSUES

1. Whether dispute as to adequacy of search for records responsive to plaintiff's Freedom of Information Act request precluded summary judgment.

2. Whether 5 U.S.C. § 552(b)(1) exempts from disclosure purportedly classified information which is in fact public knowledge.

3. Whether it was error for the District Court to uphold agency claims of exemption under 5 U.S.C. § 552(b)(1), (2), (7)(C), (7)(D), and (7)(E) on the basis of vague, conclusory, and false government affidavits, and without allowing plaintiff to conduct any discovery.

4. Whether an agency can properly excise information under 5 U.S.C. § 552(b)(7) where the records sought were not compiled for law enforcement purposes.*

STATUTES AND REGULATIONS

The Freedom of Information Act, 5 U.S.C. § 552, provides in pertinent part:

> (b) This section does not apply to matters that are--
>
> (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
>
> (2) related solely to the internal personnel rules and practices of an agency;
>
> * * *
>
> (7) investigatory records compiled for law enforcement purposes, but only to the extent that the production of such records would *** (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source and, in the case of a rec-

---

*This case has not previously been before this Court, or any other Court (other than the Court below), under this or any other title.

> ord compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source, (E) disclose investigative techniques or procedures ***

Because of their length, Executive order 11652, Executive order 12065, and the National Security Council directive of May 19, 1972 implementing E.O. 11652 are set forth in the addendum to this brief.

REFERENCES TO PARTIES AND RULINGS

The parties to this litigation are Harold Weisberg, plaintiff-appellant, and Clarence M. Kelley, Hon. Griffin Bell, and the United States Department of Justice, defendants-appellees.

On February 15, 1979, United States District Court Judge John Lewis Smith awarded summary judgment to the defendants. His opinion is found at pages 269-272 of the Appendix. On March 29, 1979, Judge Smith entered an order denying plaintiff's motion for reconsideration. [App. 530]

STATEMENT OF THE CASE

A. Background

On May 23, 1966 plaintiff Harold Weisberg ("Weisberg") wrote then-FBI Director J. Edgar Hoover a letter suggesting that there were at least five bullets involved in the assassination of Pres-

ident Kennedy rather than the three alleged by the Warren Commission. He brought to Hoover's attention certain matters which he believed "require immediate unequivocal explanations," and he called upon Hoover to make "immediately available" the spectrographic analysis which the FBI had performed upon the intact bullet alleged to have wounded both President Kennedy and Governor Connally and upon various bullet fragments said to have been connected to the shooting. A June 6, 1966 memorandum from Alex Rosen to Cartha DeLoach recommended "[t]hat Weisberg's communication not be acknowledged." See Exhibit 2 to 2/21/79 Weisberg Affidavit. [App. 439] It never was.

After the Freedom of Information Act ("FOIA") became effective on July 1, 1967, Weisberg submitted numerous requests to the FBI for information pertaining to the assassinations of President Kennedy and Dr. Martin Luther King, Jr. Years passed without any response to his requests.

On December 6, 1977, Weisberg received a letter from Mr. Allen McCreight, Chief, Freedom of Information/Privacy Acts Branch, Records Management Division, Federal Bureau of Investigation, in which McCreight informed him--for the first time--that on December 7, 1977 the FBI would be releasing the first of two segments of Headquarters records on the assassination of President Kennedy, and that the two segments together would total approximately 80,000 pages.

In replying to McCreight, Weisberg pointed out that he had filed "two dozen or more" FOIA requests for records on President

Kennedy's assassination but that there had been no compliance. In addition to soliciting "any explanation you would care to provide for this persisting non-compliance," Weisberg made a new information request which asked for:

1. All worksheets related to the processing of FBI Headquarters records on the assassination of President Kennedy;

2. All other records related to the processing, review, and release of these records;

3. Any other records which indicated the content of FBI Headquarters records on the assassination of President Kennedy, and,

4. Any separate list or inventory of FBI records on President Kennedy's assassination not yet released. [App. 55]

On February 13, 1978, there having been no response to his December 6, 1977 FOIA request, Weisberg filed suit in District Court.

A week after Weisberg filed suit, the Department of Justice replied to his January 19, 1978 appeal. Writing in the name of Acting Deputy Attorney General Benjamin Civiletti, Mr. Quinlan J. Shea, Jr., Director of the Office of Information and Privacy Appeals, informed Weisberg that:

> Even prior to the receipt of your letter of January 19, I had been discussing with the Bureau the matter of the possible release of its worksheets; that was in the general sense--not just the Kennedy case--and resulted from my testimony before the Abourezk Subcommittee late last year. At that time, former Deputy Attorney General Flaherty and I assured the Subcom-

> mittee that we would give serious attention to the problem of giving requesters more information, at the initial stage, about the nature and quantity of records to which access is denied. ***
>
> With respect to the actual Kennedy assassination worksheets, it may possibly turn out not to be necessary for me to act formally. The Bureau is still considering whether to put "clean" copies of the final version of these items into the reading room and otherwise to make them available to interested persons. [App. 11]

By letter dated March 6, 1978, Chief McCreight responded to Weisberg's December 6, 1977 FOIA request, telling him: "Please be assured that we are making every effort to process your request promptly." [App. 13] On April 12, 1978, McCreight sent Weisberg "2,581 pages of inventory worksheets utilized in the processing of files pertaining to the investigation into the Assassination of President John F. Kennedy." [App. 57] However, no records other than these worksheets were provided.

B. Proceedings in District Court

1. Government's Motion to Dismiss/Summary Judgment

On April 18, 1978, the government told the District Court that "defendants will move for summary judgment within the next thirty (30) days." The thirty days, it asserted, "is necessary in order that defendants might be afforded an opportunity to prepare proper affidavits." It also mentioned the workload of government counsel."

Two and a half months later, on July 3, 1978, the government filed a motion to dismiss or, alternatively, for summary judgment. The motion was supported by the affidavits of two FBI Special Agents, David M. Lattin and Horace P. Beckwith. Both affidavits were executed on April 28, 1978; both consisted largely of familiar FBI boilerplate. Beckwith's affidavit primarily dealt with excisions made on the worksheets on the basis of Exemptions 2, 7(C), 7(D) and 7(E). In large measure it was identical in content and language to the affidavit he had executed just eleven days earlier, on April 17, 1978. A key paragraph, identical to one in his earlier affidavit, asserted that:

> (7) The release of these inventory worksheets is pursuant to plaintiff's request for records relevant to the processing and release of the original records. <u>These worksheets represent the only documents available within the FBI which are responsive to plaintiff's request</u>.

(Emphasis added) [App. 54]

The Lattin Affidavit attempted to justify, in extremely vague and conclusory language, 19 excisions made on the worksheets under Exemption 1. All 19 excisions were said to be classified "confidential." Lattin swore that he had determined that "the proper classification has been assigned and that they have been appropriately marked in accordance with EO 11652 and Section 4(A), and 28 C.F.R. 17.40, <u>et seq</u>." Lattin Affidavit, ¶9. [App. 49]

Of the 19 classified items on the worksheets, Lattin stated that 13 were classified because they would "reveal cooperation with foreign police agencies." Lattin Affidavit, ¶6. [App. 46] Four items

were allegedly classified because they "could identify an intelligence method," one which Lattin described as "a method that was directed at establishments of foreign governments within the United States." Lattin Affidavit, ¶7. [App. 46] Finally, two of the items were purportedly classified because they would identify intelligence sources. According to Lattin, "[b]oth of these sources are foreign nationals having contacts with foreign establishments or individuals in foreign countries." Lattin Affidavit, ¶8. [App. 47-48]

Lattin did not state that he had examined the underlying documents, i.e., the FBI documents from which the "classified" information on the worksheets had been extracted, and he did not state that the underlying documents were actually properly classified under E.O. 11652. Nor did he state that the "classified" information on the worksheets was not already a matter of public knowledge.

2. Plaintiff's Opposition

On August 2, 1978, plaintiff filed an Opposition to the government's motion to dismiss/summary judgment. The Opposition was supported by two lengthy affidavits by Harold Weisberg, dated July 10 and July 19, 1978, and numerous exhibits. The Opposition and these supporting materials disputed the government's contentions as to the adequacy of the search for records responsive to the request and all claims of exemption for the excisions made on the worksheets.

3. Plaintiff's Attempts to Exercise Discovery

On August 16, 1978, plaintiff noted the depositions of FBI Agents Allen H. McCreight and Horace P. Beckwith and issue a subpoena duces tecum requiring them to bring certain records with them. The notice of deposition specified that the depositions would be taken on August 30, 1978. However, the day before the depositions were to be taken, Weisberg's counsel was told, upon phoning defendants' attorney, that Agents Beckwith and McCreight would not appear and that the government was filing a motion to quash the depositions. Consequently, no depositions were taken.

On October 4, 1978, Weisberg again noted the depositions of Beckwith and McCreight, this time for October 31, 1978. No subpoena duces tecum was issued in connection with this deposition. On October 16, 1978, the government again moved for a protective order, asserting that the court should act on pending dispositive motions prior to any discovery, and that the depositions "would indeed be burdensome and possibly a waste of resources." Defendant's 10/16/78 Memorandum in Support of Motion for a Protective Order, p. 3. [App. 210]

On October 25, 1978, the District Court issued an order granting the Motion for a Protective Order. The Court made no findings and stated no grounds for its order. [App. 215]

4. Oral Argument

On January 10, 1979, oral argument was held on the government's Motion to Dismiss/Summary Judgment. At oral argument Weis-

berg pointed out that E.O. 12065, the new Executive order governing national security classification, had become effective on December 1, 1978. He argued that because E.O. 12065 significantly changed the security classification standards, the determinations made by Special Agent Lattin under E.O. 11652 were no longer valid.

On January 12, 1979, the District Court ordered the government to submit within ten days "an affidavit by the appropriate person regarding classification status under Executive Order 12065 of those documents at issue in this action previously classified pursuant to Executive Order 11652." His order also gave Weisberg just five days to respond to the government's new security classification affidavit. [App. 248]

On January 22, 1979, the government filed an affidavit by FBI Special Agent Bradley B. Benson which asserted that the information previously said to have been properly classified under E.O. 11652 was also classified under E.O. 12065.

Weisberg's counsel did not receive a copy of the Benson affidavit until January 25, 1979. The following day he filed a motion for an extension of time in which to respond to the Benson affidavit. In the motion he represented that he had mailed a copy of the affidavit to Weisberg the day he received it, but that Weisberg might not get it until January 29th; that Weisberg would undoubtedly want to file a counteraffidavit, but that he had been unable to reach him by phoning him at his Frederick, Maryland home; that Weisberg should be allowed several days to check his own records and to prepare a counteraffidavit; and that he himself would

be working for the next several days to complete a brief due in the Court of Appeals in another Weisberg case.

The District Court granted the motion for an extension of time to and including February 8, 1979. On February 9, 1979, Weisberg moved for a further extension of time, to and including February 17, 1979, within which to respond to the Benson affidavit. Weisberg's counsel represented to the Court that Weisberg had nearly completed his counteraffidavit, but that he suffered from circulatory problems and had not been feeling well; that in recent weeks he had passed out on one occasion and had nearly done so again "only last week"; that he had been forced to take time out to see his physician and to undergo medical testing; and that because of his personal situation, he had also had to spend time battling to keep his 100-yards long country lane free of ice and snow. The motion concluded by noting that, weather and health permitting, Weisberg would be coming to D.C. on February 13, 1979, to hear oral argument in the Court of Appeals on one of his cases, and that at that time he should be able to furnish his counsel with a completed draft of his affidavit. He requested an additional four days after this date so his counsel could make any necessary revisions in the affidavit and draw up a memorandum to accompany it.

On February 12, 1979, the District Court denied the motion for a further extension of time in which to respond to the affidavit of Special Agent Benson. [App. 268]

5. District Court's Opinion

On February 15, 1979, the District Court issued an Opinion and an order granting summary judgment in favor of the government. [App. 269-272] The Opinion recited that Weisberg "seeks the disclosure of worksheets and records relating to the processing, review and release of the material on the assassination of President Kennedy made public by the Federal Bureau of Investigation on De- 7, 1977 and thereafter." (Emphasis added) [App. 269] Although only worksheets had been provided Weisberg, the District Court made no finding as to whether an adequate search--or any search at all--had been made for other records relevant to his request.

With respect to Exemption 1, the District Court found that "the FBI affidavits show that the documents are classified according to the proper procedural criteria and that they are correctly withheld under both Executive Orders 11652 and 12065." Relying upon Weissman v. CIA, 184 U.S.App.D.C. 117, 565 F.2d 692 (1977), and the fact that the legislative history of the Freedom of Information Act contains a statement that "substantial weight" is to be accorded to agency affidavits setting forth the basis for claims of exemption under 5 U.S.C. § 552(b)(1), the Court found that Weisberg had made no showing of lack of good faith on the part of the FBI, and that "[t]he defendants have sustained their burden of showing that the withheld material is protected from disclosure under Exemption 1." [App. 270]

With respect to Exemption 2, the District Court found that the deletion of informant file and symbol numbers was related to

the internal practices of an agency, that release of these numbers "could result in the disclosure of the identity of the informant, protected under 7(D)," and that "[i]t is obvious that the public's interest in knowing the names of FBI informants is neither significant nor genuine when compared with the FBI's need to keep this information confidential." Therefore he found that "the numbers utilized by the FBI have been properly withheld pursuant to Exemptions 2 and 7(D)." [App. 270]

In regard to Exemption 7(C), the Court found that the government had invoked it "to withhold the names, background data and other identifying information involving third parties as well as the names of FBI agents who produced the worksheets." Asserting that the withheld information "pertains to individuals coming to the attention of the FBI who were not the subject of the investigation," the Court held that "[t]he public interest in disclosing this information does not outweigh the privacy interests of these individuals." [App. 271]

Turning to Exemption 7(D), the Court asserted that the government had invoked it "to withhold the identity of confidential informants and the information supplied by them." He went on to construe the phrase "confidential source" as used in Exemption 7(D) to include "any source whether it be an individual, an agency or a commercial or institutional source." On this basis he ruled that all material withheld under 7(D) is exempt from disclosure. [App. 272]

Finally, with respect to Exemption 7(E), the Court stated that the FBI had asserted it "to protect two investigative techniques from disclosure." On the basis of this meagher assertion, the Court conlcuded only that "[t]his is consistent with the purpose of the exemption." [App. 272]

The Court made no finding that any of the information sought by Weisberg had been "compiled for law enforcement purposes," as required by Exemption 7.

6. Motion for Reconsideration and Clarification

On February 16, 1979, Weisberg filed a Motion for Reconsideration and Clarification Pursuant to Rules 52(b) and 59 of the Federal Rules of Civil Procedure. The motion was supported by three affidavits by Weisberg and numerous exhibits. Weisberg had originally intended to file one of these affidavits--the one executed on February 14, 1979--in opposition to the Benson Affidavit. However, because the District Court refused to give Weisberg a few more days to complete his counteraffidavit, even though counsel had represented to the Court that he was in ill health, the affidavit was filed after the Court's decision rather than before it.

The Motion for Reconsideration provided new materials bearing directly on the government's claims and the Court's findings. For example, on the issue of whether he had been provided all materials within the scope of his request, Weisberg provided incontrovertible documentary evidence of another set of worksheets, differing in many particulars from the one provided to him but in-

tended to describe the same records. This different set of worksheets had been sent to a different requestor on October 8, 1977, a month prior to Weisberg's FOIA request. See 2/21/79 Weisberg Affidavit, ¶¶47-51, 70 [App. 412-412, 417]; Exhibits 6-7 [App. 454-455].

The Benson Affidavit marked the first time that the government had identified any excisions in a way which made it possible to locate them on the 2,581 pages of worksheets. While this itemization was limited to the 19 excisions allegedly based on national security grounds, it did make it possible for Weisberg to check Benson's representations concerning these excisions with the underlying documents or routing slips which referred to them.

The materials attached to Weisberg's February 14 affidavit, garnered as a result of the time-consuming check he made, showed that many, if not most, of the excisions made under Exemption 1 consisted of masking the initials "RCMP," standing for "Royal Canadian Mounted Police." The documents produced by Weisberg also established that the cooperation of the Royal Canadian Mounted Police with the FBI in the investigation of the assassination of President Kennedy had already been disclosed by the FBI's release of routing slips with this information on them. See 2/14/79 Weisberg Affidavit, ¶¶66-70 [App. 298-299]; Exhibits 12-14 [App. 346-348].

In addition, Weisberg swore that the fact that the Mounties had cooperated with the FBI during the investigation of the President's assassination had long been public knowledge; that this

information is available in the National Archives; and that Weisberg had himself published records showing the cooperation of the Mounties and the FBI. See 2/14/79 Weisberg Affidavit, ¶¶99-107. [App. 306-309]

Weisberg's Motion for Reconsideration also pointed out that Benson's affidavit made it apparent that the worksheets had not been classified until after he filed suit for them. Because Executive Order 11652 provided that classification was to occur at the time of origination, this disclosure contradicted the Lattin Affidavit, which swore that the proper classification procedures under E.O. 11652 had been followed.

On March 22, 1979, Weisberg filed a motion to vacate the Protective Order which the Court had issued on October 25, 1979. At the same time, he also filed a motion for a Vaughn v. Rosen index.

The government filed an Opposition to the Motion for Reconsideration on March 22nd. On March 29th the District Court denied the Motion for Reconsideration. [App. 530]

SUMMARY OF ARGUMENT

This is a Freedom of Information Act lawsuit for all worksheets related to the processing of FBI Headquarters records on the assassination of President Kennedy; all other records relating to the processing, review, and release of these records; and any inventories of JFK assassination records. The FBI claimed that

the only records responsive to the request were 2,581 pages of worksheets which it released to plaintiff Weisberg. However, Weisberg established by documentary evidence that other records exist which come within the scope of his request, including other sets of inventory worksheets. These records were not provided. The District Court made no finding as to whether all records within the scope of the request had been provided, nor did he rule on the adequacy of the search which was made for such records. Because an agency must prove in a FOIA case that each document which falls within the class requested either has been produced, is unidentifiable, or is wholly exempt, summary judgment is improper. National Cable Television Association v. F.C.C., 156 U.S.App.D.C. 91, 1974, 479 F.2d 186 (1973).

The government claimed that certain excisions made on the worksheets were justified under Exemption 1. The District Court, erroneously relying upon Weissman v. CIA, 184 U.S.App.D.C. 117, 565 F.2d 692 (1977), which had previously been substantially modified by Ray v. Turner, 190 U.S.App.D.C. 290, 587 F.2d 1187 (1978), and giving conclusive weight to the FBI's affidavits, upheld the government's claims. However, Weisberg demonstrated by documentary evidence that many, if not most of the materials deleted under Exemption 1 consisted of nothing more than the initials "RCMP", standing for "Royal Canadian Mounted Police", that cooperation between the Mounties and the FBI during the investigation of President Kennedy's assassination had been public for years, and that the FBI itself had already released the withheld information.

In addition, despite deceptively worded FBI affidavits to the contrary, the proper classification procedures were not followed. In violation of the procedures required by E.O. 11652, as implemented by the National Security Council Directive of May 17, 1972, and the Justice Department's own regulations, the worksheets were not classified until several months after Weisberg's FOIA request. The failure to follow classification procedures prescribed by Executive order, including the time of classification, can compel disclosure. Schaffer v. Kissinger, 164 U.S.App. D.C. 282, 505 F.2d 389 (1974). Where proper classification procedures have not been followed and the government alleges that disclosure would constitute a grave danger to national security, the District Court should examine the materials in camera to determine whether they may be withheld according to the exacting standard employed in First Amendment cases involving prior restraint. Halperin v. Department of State, 184 U.S.App.D.C. 124, 131-132, 565 F.2d 699, 706-707; Ray v. Turner, 190 U.S.App.D.C. 290, 318, 587 F.2d 1197, 1215, note 62 (concurring opinion of Chief Judge Wright).

Because materials which are already publicly known cannot be properly classified according to the substantive criteria of either E.O. 11652 or E.O. 12065, the "RCMP" excisions must be restored. The government's conclusory affidavits do not provide an adequate basis for awarding summary judgment with respect to any other Exemption 1 excisions. Moreover, under E.O. 12065 even if the unauthorized disclosure of information would result in identifiable

harm to the national security, such information is protected by Exemption 1 only if that identifiable harm is not outweighed by the public interest in disclosure. The affidavit of the FBI Special Agent who examined the Exemption 1 excisions under the provisions of E.O. 12065 fails to recite that he made this determination.

The District Court also upheld the government's excision of informant symbol and file numbers under Exemption 2, ruling that these numbers "relate to the internal practices of an agency." This ruling is defective in two regards. First, it does not assert that these numbers relate solely to such practices, even though this is plainly a requirement of the law. Secondly, it has been held that in the phrase "internal personnel rules and practices of an agency", the phrase "internal personnel" modifies both "rules" and "practices". Jordan v. United States Dept. of Justice, 192 U.S.App.D.C. 144, 155, 591 F.2d 764 (1978). The FBI made no showing that the informants represented by the excised symbol and file numbers were FBI personnel. Weisberg provided documentary evidence of one FBI informant covered by a symbol number who was required to sign a statement that he was not an FBI employee.

Because the disclosure of informant file and symbol numbers does not reveal the names or identities of informants, there is no harm to governmental interests. On the other hand, there is a genuine and substantial public interest in the disclosure of these numbers because they provide a means of evaluating the content and

significance of events and information. They also enable an evaluation of the FBI's performance in its investigation of President Kennedy's assassination. On balance the public interest in disclosure clearly predominates. Thus, even if such numbers fall within the purview of Exemption 2, they must be disclosed.

The government also made excisions on the worksheets under Exemptions 7(C), (D), and (E). Weisberg contends that this Exemption is inapplicable because the government did not make a required preliminary showing that the FBI compiled these records for "a law enforcement purpose." In this regard he notes that FBI Director J. Edgar Hoover testified before the Warren Commission that there was no Federal jurisdiction to investigate the assassination of the President, and that the Warren Commission stated it had no law enforcement purposes.

The FBI excised the names of the FBI agents who prepared the inventory worksheets on the grounds that the release of their names "could cause public exposure or harassment of Special Agents and their families . . . ." These excisions are unjustifiable and the reason advanced for them is preposterous. FBI agents "have no legitimate privacy right to deletion of their names. Their involvement in investigative activities for the FBI is not a 'private fact'." Ferguson v. Kelley, 448 F.Supp. 919, 923 (N.D.Ill. 1977) Moreover, the overriding public interest in the fullest possible disclosure of information about the assassination of President Kennedy would have to be given substantial weight in balancing privacy considerations against the public interest were any valid

privacy interest really presented.

With respect to 7(C) excisions made to protect the names and other identifying information on third parties, the District Court failed to take into account the overriding public interest in disclosure of information about the Kennedy assassination and the obvious liklihood that most such information in FBI files has already been publicly disclosed through books, the news media, congressional hearings and the like. The FBI made no claim that its 7(C) excisions do not include information already publicly known. In addition, in view of the numerous examples Weisberg adduced of the FBI's inconsistent application of 7(C), the refusal of the District Court to allow him to undertake discovery and the failure of the FBI to provide a Vaughn v. Rosen-type index made summary judgment inappropriate.

The FBI's invocation of 7(D) presents similar issues. The government failed to make any showing that information withheld under this claim of exemption was confidential or that there was an agency promise or implicit agreement to hold the matter in confidence. Rural Housing Alliance v. U.S.Dept. of Agriculture, 162 U.S.App.D.C. 122, 498 F.2d 73 (1974); Local 32 v. Irving, 91 LRRM 2513 (W.D.Wash. 1976). In addition, the FBI made no claim that the information excised under 7(D) was not already public domain and it did not provide an index and itemization of these excisions. Consequently, there was not a sufficient basis upon which to base an award of summary judgment.

The District Court's ruling that the phrase "confidential source" as used in 7(D) applies to an agency or a commercial or institutional source is clearly wrong since the legislative history of the Act shows that it was intended to refer only to human sources.

The FBI also deleted information on the worksheets under Exemption 7(E) because it would reveal "investigative techniques and procedures." The legislative history of 7(E) shows that it is not intended to apply to matters which are already publicly known. See Conference Report, H.Rep.No. 93-1380, 93d Cong., 2d Sess. 13 (1974). The FBI failed to state that the investigative techniques it excised are not publicly known. Accordingly, summary judgment was improperly granted with respect to these claims also.

ARGUMENT

I. SUMMARY JUDGMENT WAS IMPROPER WHERE ADEQUACY OF SEARCH FOR DOCUMENTS RESPONSIVE TO FOIA REQUEST WAS IN DISPUTE

A motion for summary judgment is properly granted only when no material fact is genuinely in dispute, and then only when the movant is entitled to prevail as a matter of law. Fed.R.Civ.P. 56(c); Adickes v. S.H. Kress & Co., 398 U.S. 144, 157 (1970); Bouchard v. Washington, 168 U.S.App.D.C. 402, 405, 514 F.2d 824

827 (1974); Nyhus v. Travel Management Corp., 151 U.S.App.D.C. 269, 271, 466 F.2d 440, 442 (1972). In assessing the motion, all "inferences to be drawn from the underlying facts contained in [the movant's] materials must be viewed in the light most favorable to the party opposing the motion." United States v. Diebold, Inc., 369 U.S. 654, 655 (1962). The movant must shoulder the burden of showing affirmatively the absence of any meaningful factual issue. Bloomgarden v. Coyer, 156 U.S.App.D.C. 109, 113-114, 479 F.2d 201, 206-207 (1973). That responsibility may not be relieved through adjudication since "[t]he court's function is limited to ascertaining whether any factual issue pertinent to the controversy exists [and] does not extend to the resolution of any such issue." Nyhus, supra, note 32, 151 U.S.App.D.C. at 271, 466 F.2d at 442.

In a Freedom of Information Act lawsuit, National Cable Television Association v. F.C.C., 156 U.S.App.D.C. 91, 94, 479 F. 2d 183, 186 (1973), this Court held that in order to prevail on a motion for summary judgment,

> the defending agency must prove that each document that falls within the class requested either has been produced, is unidentifiable, or is wholly exempt from the Act's inspection requirements.

In this case Weisberg seeks:

1. All worksheets related to the processing of FBI Headquarters records on the assassination of President Kennedy;

2. All other records related to the processing, review, and release of these records;

3. Any other records which indicated the content of FBI Headquarters records on the assassination of President Kennedy, and,

4. Any separate list or inventory of FBI records on President Kennedy's assassination not yet released.

The government provided Weisberg with a set of worksheets said to total 2,581 pages. It then submitted an affidavit by FBI Special Agent Horace P. Beckwith which asserted that: "These worksheets represent the only documents available within the FBI which are responsive to plaintiff's request." 4/17/78 Beckwith Affidavit, ¶4. [App. 25]

Agent Beckwith has been used extensively as an affiant in Weisberg's FOIA cases. He has been publicly reported as being an unindicted co-conspirator in FBI illegalities. See 7/10/78 Weisberg Affidavit, ¶¶16-19. [App. 99-101] This alone militates against giving any credence to his affidavits. In addition, however, he has misrepresented critical facts in other FOIA cases. Thus, as a result of an affidavit which Agent Beckwith submitted in Lesar v. Department of Justice, Civil Action No. 77-0692 (now pending in this Court as Case No. 78-2305), Weisberg learned that in another case, Weisberg v. Department of Justice, Civil Action No. 75-1996, Beckwith ad misrepresented two Atlanta Field Office serials on the assassination of Dr. King as consisting of 2 pages, neither of which was withheld, when in fact they consisted of 29 pages, 27 of which had been withheld without Weisberg's knowledge. See 7/10/78 Weisberg Affidavit, ¶19 [App. 99]; Exhibit 2 [App. 128].

In this case, Agent Beckwith has again misrepresented the facts. The worksheets provided Weisberg were not "the only documents available within the FBI which are responsive to [his] request." Indeed, they are not even the only set of worksheets responsive to his request. For example, a different set of worksheets, one which did not itemize the identical underlying records and which contained improper obliterations, was sent to another requester, a Mr. Paul Hoch. Comparison of the Hoch worksheets with those sent to Weisberg reveals "different entries, different handwriting, different information and other differences, even though both sets are dated July, 1977." 2/21/79 Weisberg Affidavit, ¶¶43-51 [App. 411-413]; Exhibits 6-7 [App. 454-455]

Nor is Beckwith's affidavit true with respect to Item 2 of Weisberg's request, which calls for "[a]ll records related to the processing, review, and release of" the FBI's Central Headquarters files on the assassination of President Kennedy. Weisberg provided evidence that such records existed when he filed his Opposition to the government's Motion to Dismiss/Summary Judgment.

For example, Weisberg noted that in connection with Weisberg v. Bell, et al., Civil Action No. 77-2155, FBI Director Clarence M. Kelley had tried to deny him a total waiver of search fees and copying costs for the FBI's Kennedy assassination records by representing to his counsel--and the District Court--that "[w]e anticipate that additional sets of documents will be produced and placed in other research facilities, such as the Library of Con-

gress, in the near future." 1/9/78 letter from Director Kelley to James H. Lesar. Opposition Attachment A. [App. 79] Three days later Office of Privacy and Information Appeals Director Quinlan J. Shea, Jr. wrote, in the name of Acting Deputy Attorney General Benjamin R. Civiletti, that in recognition of the historical importance of the FBI's records on President Kennedy's assassination, "Director Kelley . . . on his own initiative, made arrangements for the released materials to be made available at a number of different public locations . . . ." 1/12/78 from Quinlan J. Shea, Jr. to James H. Lesar. Opposition Attachment B. [App. 81]

Unless these representations were false--and it bears repeating that they were made to United States District Judge Gerhard Gesell, as well as to Weisberg's counsel--then the FBI should have records relating to the decision to place these documents in other locations, such as the Library of Congress, as well as records reflecting those locations actually selected, the conditions under which the recipients got them, and the arrangements for their actual transmittal. No such records were provided to Weisberg.

It is also obvious that the decision to place a set of these Kennedy assassination records in the FBI reading room did not spring from the head of Director Kelley as did Athena from the head of Zeus, full-grown, in complete armor, and with a might war-whoop. Such a decision would not be made without discussions and memoranda on whether this project should be undertaken, as well as the costs and mechanics of doing it. One example of this kind

of record is the November 17, 1977 memorandum from A. J. Decker to Mr. McDermott which discusses the costs involved in processing the "approximately 600 sections" of FBI records which comprise the JFK assassination files. Opposition Attachment C. [App. 83] It was not provided to Weisberg in response to the FOIA request which is the subject of this lawsuit, although it should have been.[1/] Nor were any other documents of this kind supplied.

The Decker memorandum states that approximately 60 FOIA requests "of various scope" had been made for FBI records on President Kennedy's assassination. These requests and the administrative records generated in response to them are clearly within the scope of Item 2 of Weisberg's request. Yet none have been provided. Also within the scope of Item 2 would be any list of FOIA requests for Kennedy assassination records. At the September 16, 1976 hearing in Weisberg v. U.S. Department of Justice, Civil Action No. 75-1996, FBI Special Agent John Howard testified that such a list was compiled. Opposition Attachment D. [App. 85] No such list has been provided to Weisberg.

Finally, Item 4 of Weisberg's request asked for "[a]ny separate list or inventory of FBI records on President Kennedy's assassination not yet released." Weisberg provided the District Court with documentary evidence that FBI Headquarters had directed all

---

1/ The Decker memorandum shows on its face that it was distributed to no less than six FBI officials, not including Decker or McDermott. It was marked to the attention of FBI Special Agent Horace P. Beckwith, who twice submitted affidavits declaring that the FBI had no records responsive to Weisberg's FOIA request except the worksheets provided him.

89 FBI field offices to provide inventories of all records relating to the assassinations of President Kennedy and Dr. King. See 2/21/79 Weisberg Affidavit, ¶¶71-73 [App. 417]; Exhibits 11-12 [App. 461, 465]. The FBI did not provide Weisberg with copies of these or other such inventories.

On this evidence it is obvious that the FBI did not produce all records responsive to Weisberg's request. It was, therefore, error for the District Court to grant summary judgment.

The District Court also abused its discretion in granting a Protective Order forbidding the taking of the depositions of FBI Agents Beckwith and McCreight. Such orders are " generally regarded by the court as both unusual and unfavorable, and most requests of this kind are denied. Grinell Corp. v. Hackett, 70 F.R.D. 326, 333-334 (1976), citing Investment Properties International, Ltd. v. Ios, Ltd., 459 F.2d 705, 708 (2d Cir. 1972). In barring Weisberg from taking these depositions, the District Court denied him the opportunity to exercise discovery on the issue of the adequacy of the search for records responsive to his request. In Association of National Advertisers, Inc. v. Federal Trade, et al., 28 Ad.L.2d 643 (D.D.C. 1976), an FOIA case in which the plaintiff challenged the adequacy of the search for responsive records, then Chief Judge Jones of the United States District Court for the District of Columbia ruled that:

> It is clear that civil discovery is a proper method for pursuing factual disputes as to the adequacy or completeness of an agency search for records requested pursuant to FOIA. See

National Cable Television Ass'n, Inc. v. FTC
479 F.2d 183, 193 (DC Cir. 1973).

It is apparent, therefore, that the District Court also committed reversible error in denying Weisberg the opportunity to depose Agents Beckwith and McCreight as to the adequacy of the FBI's search for records responsive to his request.

II. DISTRICT COURT COMMITTED ERROR IN AWARDING SUMMARY JUDGMENT TO GOVERNMENT ON EXEMPTION 1 CLAIMS

Exemption 1 of the Freedom of Information Act excludes from its mandatory disclosure requirements matters that are--

> (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order

The government filed affidavits by three different FBI agents alleging that information on the worksheets provided to Weisberg had been excised in the interests of national security. The District Court found that "the FBI affidavits show that the documents are classified according to the proper procedural criteria and that they are correctly withheld under both Executive Orders 11652 and 12065." In addition, the Court ruled that "[t]here has been no showing of lack of good faith on the part of the FBI." [App. 270]

A. District Court Erroneously Relied on Weissman v. CIA

In making its determination, the District Court erroneously relied upon Weissman v. CIA, 184 U.S.App.D.C. 117, 565 F.2d 692

(1977), which was substantially modified, if not in fact overturned by Ray v. Turner, 190 U.S.App.D.C. 290, 587 F.2d 1187 (1978), a decision which this Court handed down nearly six months prior to the District Court's ruling in this case.

B. District Court Misconstrued Weight Required To Be Given To Agency Affidavits

In holding that the government was entitled to summary judgment on its Exemption 1 claims because the legislative history "clearly indicates that substantial weight is to be accorded to agency affidavits setting forth the basis for exemption under subsection (b)(1)," the District Court relied upon a passage in the Conference Report on the 1974 Amendments to the Freedom of Information Act which states:

> . . . the conferees recognize that the Executive departments responsible for national defense and foreign policy matters have unique insights into what adverse effects might occur as a result of public disclosure of a particular classified record. Accordingly, the conferees expect that Federal courts, in making de novo determinations in [Exemption 1] cases . . . , will accord substantial weight to an agency's affidavit concerning the details of the classified status of the disputed record.

H.R. Rep. No. 1380, 93d Cong., 2d Sess. 12 (1974)

The District Court misconstrued the suggestion of the conferees that "substantial weight" be accorded agency affidavits directed at establishing Exemption 1 claims. He gave no consideration whatsoever to Weisberg's detailed and carefully documented counteraffidavits. He gave conclusive weight to the FBI's affida-

vits, even though they were highly conclusory at best and deliberately deceptive at worst. This is not what the conferees intended when they stated that they expected the courts to give "substantial weight" to agency affidavits dealing with the classified status of withheld information. As one commentator has written:

> This suggestion by the conferees is merely a reminder that those within the executive branch authorized to make security classifications will often be in a better position to evaluate the need for classification than the party seeking disclosure. The conferees have not suggested that the evidence of the party seeking disclosure should be afforded any less "substantial weight." In fact the legislative history indicates that it was Congress' intent that the evidence of both parties be accorded equal weight, commensurate with the degree of expertise, credibility, and persuasiveness underlying it. More fundamentally, the "substantial weight" suggestion of the conferees should in no way be taken to suggest the imposition of a presumption favoring the agency. President Ford vetoed the Act because he felt the conferee language failed to create such a presumption; Congress, in its initial consideration of the 1974 amendments, specifically rejected a similar presumption contained in the Senate draft of the bill. (Emphasis added) (Citations omitted)

Howard Roffman, Commentary, "Freedom of Information: Judicial Review of Executive Security Classifications," 28 University of Florida Law Review 551, 558-559 (Winter 1976).

For the District Court to give the FBI affidavits conclusive weight was improper. Given the nature of the FBI affidavits and the totality of the circumstances which had been laid before the

District Court, according them "substantial weight" was also improper. As Chief Judge Wright stated in his concurring opinion in Ray v. Turner:

> An affidavit explaining in detail the factors about particular material that have convinced the agency that the material should be classified should and will be quite influential with a reviewing court. On the other hand, an affidavit stating only in general or conclusory terms why the agency in its wisdom has determined that the criteria for nondisclosure are met should not and cannot be accorded "substantial weight" in a de novo proceeding. To substitute a presumption favoring conclusory agency affidavits for the court's responsibility to make a de novo determination with the burden on the government would repeal the very aspects of the 1974 amendments that made it necessary for the Congress to override the President's veto. (Emphasis in original)

Ray v. Turner, supra, 190 U.S.App.D.C. at 316-317, 587 F.2d at 1213-1214.

C. Withheld Information Was Not Classified in Accordance With Procedural Requirements of E.O. 11652

The affidavits which the FBI submitted in support of its Exemption 1 claims were deliberately worded to give the false impression that, as required by Exemption 1, the withheld information on the worksheets was classified in accordance with the procedural requirements of E.O. 11652. The District Court expressly ruled that this information was classified "according to the proper procedural criteria." [App. 270]

The first FBI affidavit to address the classified status of the information on the worksheets was the April 17, 1978 affidavit

of FBI Special Agent Horace P. Beckwith, which stated:

> [Exemption 1] exempts from disclosure information which is currently and properly classified pursuant to Executive Order 11652. This information contained in the inventory worksheets in the form of notations and short phrases is identical to information which is duly classified in the original documents. This information, if released, would identify foreign sources or sensitive procedures, thereby jeopardizing foreign policy and the national defense. 4/17/78 Beckwith Affidavit, ¶3(a). [App. 24]

The Beckwith Affidavit thus gives the clear impression that certain "notations and short phrases" appearing on the worksheets had already been classified in that form, as well as in the underlying "original documents." But if the January 22, 1979 affidavit of FBI Special Agent Bradley B. Benson is correct, this impression is entirely false, since Benson swears that the information on the worksheets was not classified until April 27, 1978, ten days after the date of the Beckwith Affidavit. Benson Affidavit, ¶10. [App. 254-261]

On April 28, 1978, FBI Special Agent David M. Lattin executed an affidavit in which he swore that:

> (9) The affidant has reviewed the worksheets and has determined that the proper classification has been assigned and that they have been appropriately marked in accordance with EO 11652 and Section 4(A), and 28 C.F.R. 17.40 et seq. [App. 49]

This, too, gives the false impression that the procedural requirements of E.O. 11652 (and Exemption 1) were followed. It is carefully worded to attain the FBI's objective of misleading both plaintiff and the District Court while avoiding outright perjury.

The Lattin Affidavit refers to Section 4(A) of E.O. 11652 because it pertains to the informational content of certain required classification markings but not to the time when classification should take place. Yet the National Security Council Directive implementing E.O. 11652 requires that: "At the time of origination, each document or other material containing classified information shall be marked with its assigned security classification and whether it is subject to or exempt from the General Declassification Schedule." (Emphasis added) Section 4(A), National Security Council Directive, 43 Fed.Reg. 10053 (May 17, 1972). Similarly, Lattin's citation to "28 C.F.R. 17.40 et seq" omits reference to 28 C.F.R. 17.14, which also provides that classification shall occur "at the time of origination." (Emphasis added)

Even prior to the enactment of the 1974 amendments to the Freedom of Information Act, this Court held that failure to comply with the classification procedures prescribed by Executive order, including the time of classification, could compel disclosure. Schaffer v. Kissinger, 164 U.S.App.D.C. 282, 505 F.2d 389 (1974). The Amended Act clearly provides that in order to qualify for nondisclosure under Exemption 1, the material withheld must be classified in accordance with both the substantive and procedural requirements of the relevant Executive order. 5 U.S.C. § 552(b)(1). The Conference Report on the 1974 amendments explicitly states that material withheld under Exemption 1 must be properly classi-

fied "pursuant to both procedural and substantive criteria contained in such Executive Order." H.Rep. No. 93-1200, 93d Cong., 2d Sess. 12 (1974). (Emphasis added)

The courts have hedged enforcing this provision of the law as it was written. However, this Circuit has held that where the proper classification procedures have not been followed and the government alleges that disclosure would constitute a grave danger to national security, the District Court should examine the materials in camera to determine whether they may be withheld according to the exacting standard employed in First Amendment cases involving prior restraint. Halperin v. Department of State, 184 U.S.App.D.C. 124, 131-132, 565 F.2d 699, 706-707; Ray v. Turner, 190 U.S.App.D.C. 290, 318, 587 F.2d 1197, 1215, note 62 (concurring opinion of Chief Judge Wright).

The Benson Affidavit states that although the worksheets dated to August, 1977, they were not classified until April 27, 1978. This is some nine months after origination and five months after Weisberg requested them. This failure to follow proper procedures requires that the District Court be reversed as to the Exemption 1 claims.

D. Withheld Information Is Not Properly Classified Under Substantive Criteria of Executive orders 11652 and 12065

The FBI's justification for withholding information on the worksheets under Exemption 1 sounds formidable. For example, in explaining the "identifiable damage" to the national security

which "could reasonably be expected" from the "unauthorized disclosure" of some of the allegedly classified information on the worksheets, Special Agent Benson declares, at paragraph (8)(a):

> If a withheld classified item identifies a foreign government source or international organization source, the item is so identified but with no further particularity. The information may not be further described without breaching the assurance of confidentiality afforded the foreign source. The revelation of either the identity of the source or the information furnished could reasonably be expected to cause identifiable damage to the national security by the curtailment of such information from foreign or international sources who demand or expect confidentiality. The revelation could harm foreign relations, cause expulsion of United States officials and precipitate a break in normal diplomatic intercourse. The revelation could cause physical harm or other personal disruption in the lives of cooperative foreign officials and their sources.

The spectre raised by such claims is enough to make all but the most hardened FOIA recidivist withdraw his information request forthwith and abjectly request that he be forgiven for his impudence. After all, what right-minded citizen merely questing after information about the way his government operates wants to cause a break in diplomatic relations or physical harm to "cooperative foreign officials"?

But it turns out that the FBI affidavits, though written to deceive judges and to intimidate them by evoking the horrific possibility that actual damage to national security might result from the release of the requested information, are purely hallucinogenic. What all this claptrap is about is withholding the initials "RCMP"--standing for "Royal Canadian Mounted Police"--under

the guise that their "disclosure" would actually harm national security.

Weisberg's February 14, 1978 affidavit establishes that the earth-shattering news that the Mounties had cooperated with the FBI in the investigation of President Kennedy's assassination had already been disclosed by the FBI itself. Moreover, it had long been public knowledge. This information is freely available at the National Archives, and Weisberg has himself published records showing this cooperation. See 2/14/79 Weisberg Affidavit, ¶¶69-70, 99-107 [App. 299, 306-309]; Exhibits 12-14 [App. 346-348].

Executive orders 11652 and 12065 both make it clear that the purpose of security classification is to protect against the "unauthorized disclosure" of official information which must be protected in the interests of national security. It is obvious that information which is already a matter of public knowledge cannot qualify for security classification under either order.

In addition, even if disclosure would result in identifiable harm to national security, under E.O. 12065 such information is protected by Exemption 1 only if that identifiable harm is not outweighed by the public interest in disclosure. The affidavit of Special Agent Benson, who purportedly examined the "classified" information on the worksheets under the provisions of E.O. 12065, fails to recite that he made this determination. Because it does not qualify for classification under the substantive criteria of either E.O. 11652 or E.O. 12065, the information on the worksheets which has been withheld under Exemption 1 must be released.

III. INFORMATION CANNOT BE WITHHELD UNDER EXEMPTION 7 WHERE RECORDS WERE NOT COMPILED FOR LAW ENFORCEMENT PURPOSES

The FBI deleted information on the worksheets on the authority of Exemption 7(C), (D), and (E). By its express terms, Exemption 7 applies only to "investigatory records compiled for law enforcement purposes." (Emphasis added) FBI Director J. Edgar Hoover, testifying before the Warren Commission, stated that there was no Federal jurisdiction to investigate the assassination of the President. Hearings Before the President's Commission on the Assassination of President Kennedy, Vol. V, p. 98. The Warren Commission explicitly stated that it had no law enforcement purposes. Report of the President's Commission on the Asssassination of President Kennedy, p. xiv. See 7/10/78 Weisberg Affidavit, ¶¶41-42. App. 105]

In Weissman v. CIA, 184 U.S.App.D.C. 117, 120, 565 F.2d 692, 695 (1977), this Court held that where the CIA had conducted an extensive investigation of an American citizen living at home, without his knowledge and without authority to do so, "[i]t cannot be contended that this activity was for law enforcement purposes."

In this case the FBI made no showing that the materials withheld under Exemption 7 were derived from "investigatory records compiled for law enforcement purposes." The District Court made no such finding. Unless and until such a showing is made, any withholding under Exemption 7 is improper.

IV. AWARD OF SUMMARY JUDGMENT WITH RESPECT TO EXCISIONS MADE UNDER EXEMPTIONS 2 AND 7(C), (D), AND (E) WAS IMPROPER

As noted above, a motion for summary judgment is properly granted only when no material fact is genuinely in dispute, and then only when the movant is entitled to prevail as a matter of law. Fed.R.Civ.P. 56(c); Adickes v. S.H. Kress & Co., 398 U.S. 144, 157 (1970); Bouchard v. Washington, 168 U.S.App.D.C. 402, 405, 514 F.2d 284, 827 (1974); Nyhus v. Travel Management Corp., 151 U.S.App.D.C. 269, 271, 466 F.2d 440, 442 (1972). In addition, on a motion for summary judgment, "[t]he court's function is limited to ascertaining whether any factual issue pertinent to the controversy exists [and] does not extend to the resolution of any such issues." Nyhus, supra, note 32, 151 U.S.App.D.C. at 271, 466 F.2d at 442.

The District Court violated these principles of summary judgment in upholding the government's claims of exemption. Exemption 1 has already been discussed in this context. A discussion of what is at issue with respect to the government's other claims of exemption follows.

A. Exemption 2

Exemption 2 excludes from mandatory disclosure matters that are: "related solely to the internal personnel rules and practices of an agency." Construing this provision in Department of the Air Force v. Rose, 425 U.S. 352 (1976), the United States Supreme Court held that: "Exemption 2 is not applicable to matters

subject to . . . a genuine and significant public interest." In so holding, the Court quoted Vaughn v. Rosen, 173 U.S.App.D.C. 187, 523 F.2d 1136 (1975) to the effect that:

> ". . . the Senate Report indicates that the line sought to be drawn is one between minor or trivial matters and those more substantial matters which might be the subject of legitimate public interest.
>
> * * *
>
> Reinforcing this interpretation is 'the clear legislative intent [of FOIA] to assure public access to all governmental records whose disclosure would not significantly harm specific governmental interests.' [Soucie v. David, 145 U.S.App.D.C. 144, 157, 448 F.2d 1067, 1080 (1971)]"

Department of Air Force v. Rose, supra, at 375.

The two affidavits of Special Agent Beckwith contain a discrepancy as to the employment of Exemption 2. The first affidavit swears that this exemption was asserted "solely to remove informant file numbers." (Emphasis added) 4/17/78 Beckwith Affidavit, ¶3(b). [App. 24] The second vows that it was used to remove "informant file numbers and informant symbol numbers." (Emphasis added) 4/28/78 Beckwith Affidavit, ¶6. [App. 52]

The District Court found that both informant file numbers and informant symbol numbers "relate to the internal practices of an agency." [App. 270] This finding is defective in two regards. First, it does not assert that they relate solely to such practices, even though this is plainly a requirement of the law. Secondly, the phrasing of Exemption 2 refers to "internal personnel

rules and practices of an agency", not "the internal practices of an agency", as the District Court would have it. In Jordan v. United States Dept. of Justice, 192 U.S.App.D.C. 144, 155, 591 F. 2d 753, 764 (1978), this Court observed that:

> . . . every court which has considered the specific language of Exemption 2 has concluded, for good and sufficient reasons, that the phrase "internal personnel" modifies both "rules" and "practices". (Citations omitted)

For reasons having to do with basic rules of English grammar, the legislative history of the exemption, and the general purpose of the Act, this Court reached the same conclusion. Ibid.

The issues which Weisberg raises in this regard are not academic. He put before the District Court evidence that the FBI had claimed Exemptions 2 and 7(D) for the file number of a known FBI informant who had signed an agreement with the FBI stating that he was not a Federal employee and would not represent himself as such. See 3/21/79 Lesar Affidavit, ¶3 [App. 504]; Attachment A [App. 507]. An informant not employed by the FBI is obviously not covered by an exemption which pertains only to the "internal personnel practices" of the agency. This raises an issue of fact as to whether the Exemption 2 claims made by the FBI in this case erroneously assert coverage for non-FBI personnel, thus precluding summary judgment.

The District Court found that release of the informant file and symbol numbers "could result in the disclosure of the identity of the informant, protected by Exemption 7(D)." [App. 270] Weisberg contends that this is another disputed factual issue which the District Court improperly resolved in awarding summary judgment.

He insists that disclosing the symbol informant number does not reveal the names or identities of informants. In addition, the FBI has not stated that the names and identities of these informants are not already known. Where the informers are publicly known, there can be no basis for invoking Exemption 2 to cover their informant file and symbol numbers, even where they are (or were) FBI employees.

The District Court also opined that, "[i]t is obvious that the public's interest in knowing the names of FBI informants is neither significant nor genuine when compared with the FBI's need to keep this information confidential." (Emphasis added) [App. 27] This does not correctly state the issue, since the disclosure of informant file and symbol numbers does not reveal the names or identities of informants. In addition, it gives no indication what factors the District Court considered in weighing the public interest. It is obvious, however, that there is a very substantial public interest in evaluating both the information provided to the FBI in regard to President Kennedy's assassination and in evaluating the FBI's performance in investigating this national tragedy. Informant symbol numbers provide a means of evaluating the content and significance of events and information. For example, if the informant represented by a particular symbol number provides information known to be false on any occasion, all information provided by him must be viewed as suspect unless more reliably confirmed. In such cases, content cannot be evaluated

apart from the informant. Yet unless the symbol number is known, it will not be possible to make this sort of evaluation. See 7/10/78 Weisberg Affidavit, Exhibit 3. [App. 143-153]

To give another example, it is obviously important to know whether the information in several FBI reports on the same subject came from a single informant or was supplied by two or more informants. Such information provides a means of ascertaining whether an informant's account is supported by information supplied by other informants or is contradicted by them. In turn, this provides a means of evaluating the actions taken or not taken by the FBI in response to information supplied by an informant. Unless the symbol informant numbers are divulged, there is no means of evaluating such considerations.

Thus there is a legitimate public interest in the disclosure of informant symbol numbers. Because disclosure of these numbers does not reveal the names or identities of informants, there is no harm to governmental interests. Thus the public interest predominates and they should be released.

B. Exemption 7(C)

Exemption 7(C) provides that the FOIA's compulsory disclosure requirements do not apply to investigatory records compiled for law enforcement purposes to the extent that their production would "constitute an unwarranted invasion of personal privacy."

The FBI purportedly utilized this information to "protect names, background data, and other identifying information of third parties that appear on the inventory worksheets and were withheld

in the original documents." It was also utilized to excise the names of the FBI agents who produced the inventory worksheets. The FBI claims that to release these names "could cause public exposure or harassment of Special Agents and their families, which is unwarranted and would inevitably affect their ability to perform their responsibilities." 4/28/78 Beckwith Affidavit, ¶6(c). [App. 52-53]

The District Court, in an entirely conclusory ruling, stated only that "[h]ere the information pertains to individuals coming to the attention of the FBI who were not the subject of investigation," and that "[t]he public interest in disclosing this information does not outweigh the privacy interests of these individuals." [App. 271]

The FBI's utilization of Exemption 7(C) is notoriously inconsistent. Drawing on his study of tens of thousands of FBI records, Weisberg has summarized the pattern:

> Where the FBI did not like these people, where they have held political views not approved by the FBI or where, as in the case of the widow Oswald, they spoke of the FBI in a manner the FBI did not like, the FBI displayed no interest in their privacy.

7/10/78 Weisberg privacy, ¶14. [App. 98-99] As an example, the FBI has released unexpurgated records of Marina Oswald's sexual dreams and acts and her comments about the married man with whom she slept. See 7/10/78 Weisberg Affidavit, ¶¶13-14 [App. 98-99]; Exhibit 1 [App. 124]

With respect to FBI Agents, however, the FBI frequently invokes "invasion of privacy" where there is none at all. In this

regard, it now claims it is an unwarranted invasion of privacy to release the names of the FBI Special Agents who processed the inventory worksheets, even though it did not excise the names of FBI agents from the worksheets which accompanied the release of records on the assassination of Dr. King. 7/10/78 Weisberg Affidavit, ¶44. [App. 106] The FBI holds the privacy of its agents in such tender regard that it even deleted the name of one Special Agent from a newspaper article! [App. 156]

Yet even with respect to the withholding of the names of FBI Special Agents, the FBI has been inconsistent. It has, for example, released lists giving the names, home addresses and home telephone numbers of FBI Agents. See 7/19/78 Weisberg Affidavit, Exhibits 1-3. [App. 191-194]

The practice of excising, albeit inconsistently, the names of FBI Special Agents appears to have begun after the Freedom of Information Act was amended in 1974. 7/10/78 Weisberg Affidavit, ¶50 [App. 107] The Warren Commission published alarge number of unexpurgated FBI reports in facsimile. "No FBI names were withheld, no names of those who gave information to the FBI were withheld from what the Commission published or what was available at the National Archives." 7/10/78 Weisberg Affidavit, ¶49. [App. 107]

It appears that the FBI's use of Exemption 7(C) is sometimes intended as harassment of FOIA litigants. The unjustifiable invocation of this and other exemptions also helps the FBI build statistics which it can use in its campaign to repeal the FOIA.

The FBI's description of what it has withheld in this case under Exemption 7(C) is not sufficiently detailed to provide a proper basis for awarding summary judgment. For example, there is

no statement by the FBI that what it has excised under 7(C) is not already in the public domain. Weisberg's experience is that the FBI withholds public information under all exemptions, but particularly under Exemption 7(C) and (D). Thus it has withheld from its records exactly the same information that Weisberg has himself published. 7/10/78 Weisberg Affidavit, ¶53. [App. 108] It is also common FBI practice to withhold from the records it releases what is contained in its own news clippings files. 7/10/78 Weisberg Affidavit, ¶54. [App. 108]

The plain fact is that after 15 years of investigations by the FBI, the Warren Commission, and several congressional committees, not to mention the countless magazine and newspaper articles, books, radio and T.V. reports that each new development has spawned, there is very little information which is not already public knowledge. Whether the FBI is withholding public information under the guise that it is protected by 7(C) is a factual issue which properly precludes summary in favor of the government at this point. The District Court erred in adjudicating this issue on an insufficient record, by not requiring the FBI to cross-index its claims of exemption to its justification for withholding, and by denying Weisberg the opportunity to take discovery on this issue.

It is apparent that the District Court failed to take into account the overriding interest in the fullest possible disclosure of information about the Kennedy assassination, as well as the fact that most such information is already public. By failing to spell out the factors that it weighed in coming to the conclusion that

privacy considerations outweigh the public interest in disclosure, the District Court provided an insufficient basis for review by this Court. Therefore, its decision must be reversed for this reason also.

Finally, the District Court was wrong as a matter of law in holding that the names of FBI Agents are properly withheld under Exemption 7(C). FBI Agents "have no legitimate privacy right to deletion of their names. Their involvement in investigative activities for the FBI is not a 'private fact'." Ferguson v. Kelley, 448 F.Supp. 919, 923 (N.D.Ill. 1977)

C. Exemption 7(D)

Exemption 7(D) protects "investigatory records compiled for law enforcement purposes" to the extent that the the production of such records would "disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation . . . confidential information furnished only by the confidential source."

The FBI justification for excising material under 7(D) affords no basis for awarding summary judgment in its favor. It proffers only two facts in support of this claim. First, it asserts that 7(D) "was cited in the inventory worksheets corresponding to the same information as excised in the original documents." 4/28/78 Beckwith Affidavit, ¶6(d). [App. 53] Since there has been no showing that the material in the "original documents" which was excised under 7(D) was properly excised under that claim, this is irrelevant. In addition, this claim makes it evident that

in processing the worksheets, the FBI simply rubber-stamped the claims of exemption which were made on the original documents at the time they were processed. Since the passage of time alone may errode a justification for withholding information, this procedure would be defective even if the FBI could show that the excisions on the original documents were proper at the time they were made, which it can't and hasn't.

Secondly, the FBI asserted that 7(D) was used to remove the symbol numbers and file numbers of informants "in order to insure protection of the identity of sources." 4/28/78 Beckwith Affidavit, ¶6(d). [App. 53] Since by the FBI's own admission these informant file and symbol numbers "are used to cover the actual identity of the informant," the release of these numbers would not "disclose the identity of a confidential source" as required by Exemption 7(D).

Moreover, under Exemption 7(D) the agency has the burden of showing that the withheld information is confidential and that there was an agency promise or implicit agreement to hold the matter in confidence. Rural Housing Alliance v. U.S. Dept. of Agriculture, 162 U.S.App.D.C. 122, 498 F.2d 73 (1974); Local 32 v. Irving, 91 LRRM 2513 (W.D. Wash. 1976). The FBI has not met that burden here. Indeed, it has not even stated that the information on the worksheets which was excised under 7(D) on the basis of similar claims on the original documents is confidential and that there was an agency promise or implicit agreement to keep it confidential. On this basis alone, summary judgment was improper.

Nor did the FBI state whether it withheld the identity of in- of institutional sources and information provided by them under the auspices of Exemption 7(D). The District Court ruled, however, that the purpose of 7(D) "would include any source whether it be an individual, an agency or a commercial or institutional source." [App. 272]

This ruling is clearly wrong. The term "confidential source" is not defined in the FOIA. However, the legislative history of the Act indicates that Congress intended it to apply to human, not institutional sources. The Senate amendment to Exemption 7 originally employed the term "informer" rather than "confidential source." In explaining the substitution, the Conference Committee said:

> The substitution of the term "confidential source" in section 552(b)(7)(D) is to make clear that the identity of a person other than a paid informer may be protected if the person provided information under an express assurance of confidentiality or in circumstances from which such an assurance could be reasonably inferred.

(Emphasis added) H.Rep. No. 93-1380, 93d Cong., 2d Sess. 13 (1974).

This makes it clear that Congress intended to broaden the term "informer", a term which refers only to persons, to include persons other than paid informers. It obviously did not contemplate that the term would be expanded to include agencies, whether state, federal or local. If this were the case, it would be possible to defeat the intent of Exemption 7(D) by transferring records from one federal agency to another under a promise of confidential-

ity. Nor did Congress contemplate that "source" would be expanded to include institutional sources.

Finally, Weisberg again notes that the government failed to provide any index correlating the claim of exemption 7(D) on particular records with the justification for withholding. Nor did the FBI state that information which is already publicly known is not being withheld under 7(D). For these reasons, the District Court's award of summary judgment as to Exemption 7(D) claims must also be reversed.

D. Exemption 7(E)

Exemption 7(E) bars compulsory disclosure of information which would reveal investigative techniques and procedures. In invoking this exemption the FBI stated only that, "[t]hese techniques and procedures were deleted in the worksheets in those instances where they were deleted in the original document." [4/28/78 Beckwith Affidavit, ¶6(e). [App. 53-54] This is irrelevant because no showing was made that the 7(E) excisions made in the original documents were proper.

The legislative history of 7(E) shows that it is not intended to apply to matters which are already publicly known. The Conference Report directly addressed this issue, commenting that:

> The conferees wish to make clear that the scope of this exception against disclosure of "investigative techniques and procedures" should not be interpreted to include routine techniques and procedures already well-known to the public, such as ballistics tests, fingerprinting, and other scientific tests or commonly known techniques.

H.Rep. No. 93-1380, 93d Cong., 2d Sess. 13 (1974)

The Beckwith Affidavit makes no claim that the investigative techniques excised from the inventory worksheets are not publicly known. Numerous investigative techniques employed by the FBI in connection with its Kennedy assassination investigation, such as electronic and mail surveillance, pretext, and the "con man" technique are all well-known and do not come within the protection afforded by 7(E). See 7/10/78 Weisberg Affidavit, ¶61 [App. 109]; 7/19/78 Weisberg Affidavit, ¶¶4-5 [App. 188-189]

Because the FBI did not provide an index of its claims of exemption and the District Court refused to allow Weisberg to engage in discovery, there was no basis upon which the District Court could properly determine that these excisions come within the scope of Exemption 7(E). Accordingly, the award of summary judgment made with respect to Exemption 7(E) excisions must also be reversed.

CONCLUSION

In a recent book by Sanford Ungar, the Washington Post reporter, he quotes the views of the Assistant Director of the Files and Communications Division and his "number one man" on a new effort to release FBI records under the terms of the Freedom of Information Act: "It's a young program. . . . We would like to see it killed in infancy." The FBI, p. 152.

If the FBI cannot kill the Freedom of Information Act outright, it can at least wage a war of attrition against it. By

refusing to conduct an adequate search for the records requested, by making baseless and inconsistent claims of exemption, by filing affidavits which are conclusory, obfuscatory, misleading, and false, the FBI can create "make-work" for its employees, increase its backlog of FOIA cases, and drive up the cost of FOIA litigation. Through the use of such tactics it can grind down FOIA litigants and those who represent them in court. These tactics an be particularly effective where the FBI finds it has allies among the district court judges. While bad decisions may be reversed on appeal, the cost and delay involved in forcing an FOIA litigant to appeal inevitably frustrate the purpose of the Freedom of Information Act, which is the prompt disclosure of nonexempt information.

It is time that some thought be given to doing something more than simply reversing the bad decisions of judges hostile to the Freedom of Information Act. The law in this circuit is sufficiently clear now that there is no excuse for this case having been handled the way it was. But unless this Court soon finds some means of disciplining agencies, judges, and government attorneys who make a mockery of the FOIA, there will be an endless subversion of it.

In this case the government has continued to withhold allegedly classified information even after Weisberg has shown that the material which was excised is a matter of public knowledge and never justified classification in the first place. This Court may want

to consider whether the circumstances of this case would warrant any of the sanctions provided by Rules 11 and 56(g) of the Federal Rules of Civil Procedure or 28 U.S.C. § 1927.

In any event, appellant Weisberg should be granted the following relief:

1. The District Court's award of summary judgment should be reversed on all counts.

2. On remand, the FBI should be required to file a Vaughn v. Rosen inventory and index.

3. On remand Weisberg should be allowed to take discovery with regard to the adequacy of the search for records responsive to his request. In addition, he should also be permitted to take discovery to determine what standards the FBI employed in asserting its clims of exemption and whether or not it withheld information which is already in the public domain.

4. On remand the District Court should be directed to conduct an inquiry into why the government continued to withhold purportedly classified information on the inventory worksheets even after Weisberg established that it was public knowledge and had already been released by the FBI itself, with a view towards determining whether this involved a violation of Federal Rule 11. If this Court considers that Judge John Lewis Smith cannot conduct an impartial inquiry into this matter because he continued to uphold the government's claim after Weisberg brought the public nature of the "classified" information to his attention, then this case

should be remanded to a different judge.

Respectfully submitted,

JAMES H. LESAR
910 Sixteenth Street, N.W., #600
Washington, D.C. 20006
Phone: 223-5587

Attorney for Appellant

A D D E N D U M

DIRECTIVE OF MAY 17, 1972

National Security Council Directive Governing the Classification, Downgrading, Declassification and Safeguarding of National Security Information

The President has directed that Executive Order 11652, "Classification and Declassification of National Security Information and Material," approved March 8, 1972 (37 F.R. 5209, March 10, 1972) be implemented in accordance with the following:

I AUTHORITY TO CLASSIFY

A. *Personal and Non-delegable.* Classification authority may be exercised only by those officials who are designated by, or in writing pursuant to, Section 2 of Executive Order 11652 (hereinafter the "Order"). Such officials may classify information or material only at the level authorized or below. This authority vests only to the official designated under the Order, and may not be delegated.

B. *Observance of Classification.* Whenever information or material classified by an official designated under A above is incorporated in another document or other material by any person other than the classifier, the previously assigned security classification category shall be reflected thereon together with the identity of the classifier.

C. *Identification of Classifier.* The person at the highest level authorizing the classification must be identified on the face of the information or material classified, unless the identity of such person might disclose sensitive intelligence information. In the latter instance the Department shall establish some other record by which the classifier can readily be identified.

D. *Record Requirement.* Each Department listed in Section 2(A) of the Order shall maintain a listing by name of the officials who have been designated in writing to have Top Secret classification authority. Each Department listed in Section 2 (A) and (B) of the Order shall also maintain separate listings by name of the persons designated in writing to have Secret authority and persons designated in writing to have Confidential authority. In cases where listing of the names of officials having classification authority might disclose sensitive intelligence information, the Department shall establish some other record by which such officials can readily be identified. The foregoing listings and records shall be compiled beginning July 1, 1972 and updated at least on a quarterly basis.

E. *Resolution of Doubts.* If the classifier has any substantial doubt as to which security classification category is appropriate, or as to whether

1a

the material should be classified at all, he should designate the less restrictive treatment.

II DOWNGRADING AND DECLASSIFICATION

A. *General Declassification Schedule and Exemptions.* Classified information and material shall be declassified as soon as there are no longer any grounds for continued classification within the classification category definitions set forth in Section 1 of the Order. At the time of origination the classifier shall, whenever possible, clearly mark on the information or material a specific date or event upon which downgrading or declassification shall occur. Such dates or events shall be as early as is permissible without causing damage to the national security as defined in Section 1 of the Order. Whenever earlier dates or events cannot be determined, the General Declassification Schedule set forth in Section 5(A) of the Order shall apply. If the information or material is exempted under Section 5(B) of the Order from the General Declassification Schedule, the classifier shall clearly mark the material to show that it is exempt and indicate the applicable exemption category. Unless impossible, the exempted information or material shall be assigned and clearly marked by the classifier with a specific date or event upon which declassification shall occur. Downgrading and declassification dates or events established in acordance with the foregoing, whether scheduled or non-scheduled, shall to the extent possible be carried forward and applied whenever the classified information or material is incorporated in other documents or material.

B. *Extracts and Compilations.* When classified information or material from more than one source is incorporated into a new document or other material, the document or other material shall be classified, downgraded or declassified in accordance with the provisions of the Order and Directives thereunder applicable to the information requiring the greatest protection.

C. *Material Not Officially Transferred.* When a Department holding classified information or material under the circumstances described in Section 3(D) of the Order notifies another Department of its intention to downgrade or declassify, it shall allow the notified Department 30 days in which to express its objections before taking action.

D. *Declassification of Material 30 Years Old.* The head of each Department shall assign experienced personnel to assist the Archivist of the United States in the exercise of his responsibility under Section 5(E) of the Order to systematically review for declassification all materials classified before June 1, 1972 and more than 30 years old. Such personnel will: (1) provide guidance and assistance to archival employees in identifying and separating those materials originated in their Departments which are deemed to require continued classification; and (2) develop a list for submission to the head of the Department which identifies the materials so separated, with recommendations concerning continued classification. The head of the originating Department will then make the determination required under Section 5(E) of the Order and cause a list to be created which identifies the documentation included

2a

in the determination, indicates the reason for continued classification and specifies the date on which such material shall be declassified.

E. *Notification of Expedited Downgrading or Declassification.* When classified information or material is downgraded or declassified in a manner other than originally specified, whether scheduled or exempted, the classifier shall, to the extent practicable, promptly notify all addressees to whom the information or material was originally officially transmitted. In turn, the addressees shall notify any other known recipient of the classified information or material.

III REVIEW OF CLASSIFIED MATERIAL FOR DECLASSIFICATION PURPOSES

A. *Systematic Reviews.* All information and material classified after the effective date of the Order and determined in accordance with Chapter 21, 44 U.S.C. (82 Stat. 1287) to be of sufficient historical or other value to warrant preservation shall be systematically reviewed on a timely basis by each Department for the purpose of making such information and material publicly available in accordance with the determination regarding declassification made by the classifier under Section 5 of the Order. During each calendar year each Department shall segregate to the maximum extent possible all such information and material warranting preservation and becoming declassified at or prior to the end of such year. Promptly after the end of such year the Department responsible, or the Archives of the United States if transferred thereto, shall make the declassified information and material available to the public to the extent permitted by law.

B. *Review for Declassification of Classified Material Over 10 Years Old.* Each Department shall designate in its implementing regulations an office to which members of the public or Departments may direct requests for mandatory review for declassification under Section 5 (C) and (D) of the Order. This office shall in turn assign the request to the appropriate office for action. In addition, this office or the office which has been assigned action shall immediately acknowledge receipt of the request in writing. If the request requires the rendering of services for which fair and equitable fees should be charged pursuant to Title 5 of the Independent Offices Appropriations Act, 1952, 65 Stat. 290, 31 U.S.C. 483a the requester shall be so notified. The office which has been assigned action shall thereafter make a determination within 30 days of receipt or shall explain the reasons why further time is necessary. If at the end of 60 days from receipt of the request for review no determination has been made, the requester may apply to the Departmental Committee established by Section 7(B) of the Order for a determination. Should the office assigned action on a request for review determine that under the criteria set forth in Section 5(B) of the Order continued classification is required, the requester shall promptly be notified, and whenever possible, provided with a brief statement as to why the requested information or material cannot be declassified. The requester may appeal any such determination to the Departmental Committee and the notice of determination shall advise him of this right.

C. *Departmental Committee Review for Declassification.* The Departmental Committee shall establish procedures to review and act within

3a.

30 days upon all applications and appeals regarding requests for declassification. The Department head, acting through the Departmental Committee shall be authorized to over-rule previous determinations in whole or in part when, in its judgment, continued protection is no longer required. If the Departmental Committee determines that continued classification is required under the criteria of Section 5(B) of the Order it shall promptly so notify the requester and advise him that he may appeal the denial to the Interagency Classification Review Committee.

D. *Review of Classified Material Over 30 Years Old.* A request by a member of the public or by a Department under Section 5 (C) or (D) of the Order to review for declassification documents more than 30 years old shall be referred directly to the Archivist of the United States, and he shall have the requested documents reviewed for declassification in accordance with Part II.D. hereof. If the information or material requested has not been transferred to the General Services Administration for accession into the Archives, the Archivist shall, together with the head of the Department having custody, have the requested documents reviewed for declassification. Classification shall be continued in either case only where the head of the Department concerned makes at that time the personal determination required by Section 5(E)(1) of the Order. The Archivist shall promptly notify the requester of such determination and of his right to appeal the denial to the Interagency Classification Review Committee.

E. *Burden of Proof for Administrative Determinations.* For purposes of administrative determinations under B., C., or D. above, the burden of proof is on the originating Department to show that continued classification is warranted within the terms of the Order.

F. *Availability of Declassified Material.* Upon a determination under B., C., or D. above that the requested material no longer warrants classification it shall be declassified and made promptly available to the requester, if not otherwise exempt from disclosure under Section 552(b) of Title 5 U.S.C. (Freedom of Information Act) or other provision of law.

G. *Classification Review Requests.* As required by Section 5(C) of the Order, a request for classification review must describe the document with sufficient particularity to enable the Department to identify it and obtain it with a reasonable amount of effort. Whenever a request is deficient in its description of the record sought, the requester should be asked to provide additional identifying information whenever possible. Before denying a request on the ground that it is unduly burdensome, the requester should be asked to limit his request to records that are reasonably obtainable. If none-the-less the requester does not describe the records sought with sufficient particularity, or the record requested cannot be obtained with a reasonable amount of effort, the requester shall be notified of the reasons why no action will be taken and of his right to appeal such decision.

IV Marking Requirements

A. *When Document or Other Material is Prepared.* At the time of origination, each document or other material containing classified in-

formation shall be marked with its assigned security classification and whether it is subject to or exempt from the General Declassification Schedule.

(1) For marking documents which are subject to the General Declassification Schedule, the following stamp shall be used:

(TOP SECRET, SECRET OR CONFIDENTIAL) CLASSIFIED
BY _____
SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS AND DECLASSIFIED ON DEC. 31 (insert year)

(2) For marking documents which are to be automatically declassified on a given event or date earlier than the General Declassification Schedule the following stamp shall be used:

(TOP SECRET, SECRET OR CONFIDENTIAL) CLASSIFIED
BY _____
AUTOMATICALLY DECLASSIFIED ON (effective date or event)

(3) For marking documents which are exempt from the General Declassification Schedule the following stamp shall be used:

(TOP SECRET, SECRET OR CONFIDENTIAL) CLASSIFIED
BY _____
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 EXEMPTION CATEGORY (§ 5B (1), (2), (3), or (4)) AUTOMATICALLY DECLASSIFIED ON (effective date or event, if any)

Should the classifier inadvertently fail to mark a document with one of the foregoing stamps the document shall be deemed to be subject to the General Declassification Schedule. The person who signs or finally approves a document or other material containing classified information shall be deemed to be the classifier. If the classifier is other than such person he shall be identified on the stamp as indicated.

The "Restricted Data" and "Formerly Restricted Data" stamps (H. below) are, in themselves, evidence of exemption from the General Declassification Schedule.

B. *Overall and Page Marking of Documents.* The overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked or stamped at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, on the back page and on the outside of the back cover (if any). To the extent practicable each interior page of a document which is not permanently bound shall be conspicuously marked or stamped at the top and bottom according to its own content, including the designation "Unclassified" when appropriate.

C. *Paragraph Marking.* Whenever a classified document contains either more than one security classification category or unclassified information, each section, part or paragraph should be marked to the extent practicable to show its classification category or that it is unclassified.

52

D. *Material Other Than Documents.* If classified material cannot be marked, written notification of the information otherwise required in markings shall accompany such material.

E. *Transmittal Documents.* A transmittal document shall carry on it a prominent notation as to the highest classification of the information which is carried with it, and a legend showing the classification, if any, of the transmittal document standing alone.

F. *Wholly Unclassified Material Not Usually Marked.* Normally, unclassified material shall not be marked or stamped "Unclassified" unless the purpose of the marking is to indicate that a decision has been made not to classify it.

G. *Downgrading, Declassification and Upgrading Markings.* Whenever a change is made in the original classification or in the dates of downgrading or declassification of any classified information or material it shall be promptly and conspicuously marked to indicate the change, the authority for the action, the date of the action, and the identity of the person taking the action. In addition, all earlier classification markings shall be cancelled, if practicable, but in any event on the first page.

(1) *Limited Use of Posted Notice for Large Quantities of Material.* When the volume of information or material is such that prompt remarking of each classified item could not be accomplished without unduly interfering with operations, the custodian may attach downgrading, declassification or upgrading notices to the storage unit in lieu of the remarking otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action, the identity of the person taking the action and the storage units to which it applies. When individual documents or other materials are withdrawn from such storage units they shall be promptly remarked in accordance with the change, or if the documents have been declassified, the old markings shall be cancelled.

(2) *Transfer of Stored Quantities Covered by Posted Notice.* When information or material subject to a posted downgrading, upgrading or declassification notice are withdrawn from one storage unit solely for transfer to another, or a storage unit containing such documents or other materials is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

H. *Additional Warning Notices.* In addition to the foregoing marking requirements, warning notices shall be prominently displayed on classified documents or materials as prescribed below. When display of these warning notices on the documents or other materials is not feasible, the warnings shall be included in the written notification of the assigned classification.

(1) *Restricted Data.* For classified information or material containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended:

"RESTRICTED DATA"

This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Its dissemination or disclosure to any unauthorized person is prohibited.

6a

(2) *Formerly Restricted Data.* For classified information or material containing solely Formerly Restricted Data, as defined in Section 142.d., Atomic Energy Act of 1954, as amended:

"FORMERLY RESTRICTED DATA"

Unauthorized disclosure subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination. Section 144.b., Atomic Energy Act, 1954.

(3) *Information Other Than Restricted Data or Formerly Restricted Data.* For classified information or material furnished to persons outside the Executive Branch of Government other than as described in (1) and (2) above:

"NATIONAL SECURITY INFORMATION"

Unauthorized Disclosure Subject to Criminal Sanctions.

(4) *Sensitive Intelligence Information.* For classified information or material relating to sensitive intelligence sources and methods, the following warning notice shall be used, in addition to and in conjunction with those prescribed in (1), (2), or (3), above, as appropriate:

"WARNING NOTICE—SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED"

V Protection and Transmission of Classified Information

A. *General.* Classified information or material may be used, held, or stored only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it. Whenever such information or material is not under the personal supervision of an authorized person, the methods set forth in *Appendix A* hereto shall be used to protect it. Whenever such information or material is transmitted outside the originating Department the requirements of *Appendix B* hereto shall be observed.

B. *Loss or Possible Compromise.* Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to a designated official of his Department or organization. In turn, the originating Department and any other interested Department shall be notified about the loss or possible compromise in order that a damage assessment may be conducted. An immediate inquiry shall be initiated by the Department in which the loss or compromise occurred for the purpose of taking corrective measures and appropriate administrative, disciplinary, or legal action.

VI Access and Accountability

A. *General Access Requirements.* Except as provided in B. and C. below, access to classified information shall be granted in accordance with the following:

(1) *Determination of Trustworthiness.* No person shall be given access to classified information or material unless a favorable determination has been made as to his trustworthiness. The determination of eligibility, referred to as a security clearance, shall be based on such investigations as the Department may require in accordance with the standards and criteria of E.O. 10450 and E.O. 10865 as appropriate.

(2) *Determination of Need-to-Know.* In addition to a security clearance, a person must have a need for access to the particular classified information or material sought in connection with the performance of his official duties or contractual obligations. The determination of that need shall be made by officials having responsibility for the classified information or material.

(3) *Administrative Withdrawal of Security Clearance.* Each Department shall make provision for administratively withdrawing the security clearance of any person who no longer requires access to classified information or material in connection with the performance of his official duties or contractural obligations. Likewise, when a person no longer needs access to a particular security classification category, the security clearance shall be adjusted to the classification category still required for the performance of his duties and obligations. In both instances, such action shall be without prejudice to the person's eligibility for a security clearance should the need again arise.

B. *Access by Historical Researchers.* Persons outside the Executive Branch engaged in historical research projects may be authorized access to classified information or material provided that the head of the originating Department determines that:

(1) The project and access sought conform to the requirements of Section 12 of the Order.

(2) The information or material requested is reasonably accessible and can be located and compiled with a reasonable amount of effort.

(3) The historical researcher agrees to safeguard the information or material in a manner consistent with the Order and Directives thereunder.

(4) The historical researcher agrees to authorize a review of his notes and manuscript for the sole purpose of determining that no classified information or material is contained therein.

An authorization for access shall be valid for the period required but no longer than two years from the date of issuance unless renewed under regulations of the originating Department.

C. *Access by Former Presidential Appointees.* Persons who previously occupied policy making positions to which they were appointed by the President, other than those referred to in Section 11 of the Order, may be authorized access to classified information or material which they originated, reviewed, signed or received while in public office. Upon the request of any such former official, such information and material as he may identify shall be reviewed for declassification in accordance with the provisions of Section 5 of the Order.

D. *Consent of Originating Department to Dissemination by Recipient.* Except as otherwise provided by Section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403, classified information or material originating in one Department shall not be disseminated outside any other Department to which it has been made available without the consent of the originating Department.

Sr

E. *Dissemination of Sensitive Intelligence Information.* Information or material bearing the notation "WARNING NOTICE—SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" shall not be disseminated in any manner outside authorized channels without the permission of the originating Department and an assessment by the senior intelligence official in the disseminating Department as to the potential risk to the national security and to the intelligence sources and methods involved.

F. *Restraint on Special Access Requirements.* The establishment of special rules limiting access to, distribution and protection of classified information and material under Section 9 of the Order requires the specific prior approval of the head of a Department or his designee.

G. *Accountability Procedures.* Each Department shall prescribe such accountability procedures as are necessary to control effectively the dissemintaion of classified information or material. Particularly stringent controls shall be placed on information and material classified Top Secret.

(1) *Top Secret Control Officers.* Top Secret Control Officers shall be designated, as required, to receive, maintain current accountability records of, and dispatch Top Secret material.

(2) *Physical Inventory.* A physical inventory of all Top Secret material shall be made at least annually. As an exception, repositories storing large volumes of classified material, shall develop inventory lists or other finding aids.

(3) *Current Accountability.* Top Secret and Secret information and material shall be subject to such controls including current accountability records as the head of the Department may prescribe.

(4) *Restraint on Reproduction.* Documents or portions of documents containing Top Secret information shall not be reproduced without the consent of the originating office. All other classified material shall be reproduced sparingly and any stated prohibition against reproduction shall be strictly adhered to.

(5) *Restraint on Number of Copies.* The number of copies of documents containing classified information shall be kept to a minimum to decrease the risk of compromise and reduce storage costs.

VII Data Index System

Each Department originating classified information or material shall undertake to establish a data index system for Top Secret, Secret and Confidential information in selected categories approved by the Interagency Classification Review Committee as having sufficient historical or other value appropriate for preservation. The index system shall contain the following data for each document indexed: (a) Identity of classifier, (b) Department of origin, (c) Addressees, (d) Date of classification, (e) Subject/Area, (f) Classification category and whether subject to or exempt from the General Declassification Schedule, (g) If exempt, which exemption category is applicable, (h) Date or event set for declassification, and (i) File designation. Information and material shall be indexed into the system at the earliest practicable date during the course

32

of the calendar year in which it is produced and classified, or in any event no later than March 31st of the succeeding year. Each Department shall undertake to establish such a data index system no later than July 1, 1973, which shall index the selected categories of information and material produced and classified after December 31, 1972.

VIII Combat Operations

The provisions of the Order and this Directive with regard to dissemination, transmission, or safekeeping of classified information or material may be so modified in connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe.

IX Interagency Classification Review Committee

A. *Composition of Interagency Committee.* In accordance with Section 7 of the Order, an Interagency Classification Review Committee is established to assist the National Security Council in monitoring implementation of the Order. Its membership is comprised of senior representatives of the Departments of State, Defense, and Justice, the Atomic Energy Commission, the Central Intelligence Agency, the National Security Council staff, and a Chairman designated by the President.

B. *Meetings and Staff.* The Interagency Committee shall meet regularly, but no less frequently than on a monthly basis, and take such actions as are deemed necessary to insure uniform compliance with the Order and this Directive. The Chairman is authorized to appoint an Executive Director, and to maintain a permanent administrative staff.

C. *Interagency Committee's Functions.* The Interagency Committee shall carry out the duties assigned it by Section 7(A) of the Order. It shall place particular emphasis on overseeing compliance with and implementation of the Order and programs established thereunder by each Department. It shall seek to develop means to (a) prevent overclassification, (b) ensure prompt declassification in accord with the provision of the Order, (c) facilitate access to declassified material and (d) eliminate unauthorized disclosure of classified information.

D. *Classification Complaints.* Under such procedures as the Interagency Committee may prescribe, it shall consider and take action on complaints from persons within or without the government with respect to the general administration of the Order including appeals from denials by Departmental Committees or the Archivist of declassification requests.

X Departmental Implementation and Enforcement

A. *Action Programs.* Those Departments listed in Section 2 (A) and (B) of the Order shall insure that adequate personnel and funding are provided for the purpose of carrying out the Order and Directives thereunder.

B. *Departmental Committee.* All suggestions and complaints, including those regarding overclassification, failure to declassify, or delay in declassifying not otherwise resolved, shall be referred to the Departmental Committee for resolution. In addition, the Departmental Committee shall review all appeals of requests for records under Section 522 of Title 5

U.S.C. (Freedom of Information Act) when the proposed denial is based on their continued classification under the Order.

C. *Regulations and Reports.* Each Department shall submit its proposed implementing regulations of the Order and Directives thereunder to the Chairman of the Interagency Classification Review Committee for approval by the Committee. Upon approval such regulations shall be published in the FEDERAL REGISTER to the extent they affect the general public. Each Department shall also submit to the said Chairman (1) copies of the record lists required under Part I.D. hereof by July 1, 1972 and thereafter quarterly, (2) quarterly reports of Departmental Committee actions on classification review requests, classification abuses and unauthorized disclosures, and (3) provide progress reports on information accumulated in the data index system established under Part VII hereof and such other reports as said Chairman may find necessary for the Interagency Classification Review Committee to carry out its responsibilities.

D. *Administrative Enforcement.* The Departmental Committees shall have responsibility for recommending to the head of the respective Departments appropriate administrative action to correct abuse or violation of any provision of the Order or Directives thereunder, including notifications by warning letter, formal reprimand, and to the extent permitted by law, suspension without pay and removal. Upon receipt of such a recommendation the head of the Department concerned shall act promptly and advise the Departmental Committee of his action.

Publication and Effective Date: This Directive shall be published in the FEDERAL REGISTER and become effective June 1, 1972.

HENRY A. KISSINGER,
Assistant to the President for National Security Affairs.

MAY 17, 1972.

APPENDIX A

PROTECTION OF CLASSIFIED INFORMATION

A. *Storage of Top Secret.* Top Secret information and material shall be stored in a safe or safe-type steel file container having a built in three-position dial-type combination lock, vault, or vault-type room, or other storage facility which meets the standards for Top Secret established under the provisions of (C) below, and which minimizes the possibility of unauthorized access to, or the physical theft of, such information or material.

B. *Storage of Secret or Confidential.* Secret and Confidential material may be stored in a manner authorized for Top Secret information and material, or in a container or vault which meets the standards for Secret or Confidential, as the case may be, established under the provisions of (C) below.

C. *Standards for Security Equipment.* The General Services Administration shall, in coordination with Departments originating classified information or material, establish and publish uniform standards, specifications and supply schedules for containers, vaults, alarm systems and associated security devices suitable for the storage and protection of all categories of classified information and material. Any Department may establish for use within such Department more stringent standards. Whenever new security equipment is procured, it shall be in conformance with the foregoing standards and specifications and shall, to the maximum extent practicable, be of the type designated on the Federal Supply Schedule, General Services Administration.

D. *Exception to Standards for Security Equipment.* As an exception to (C) above, Secret and Confidential material may also be stored in a steel filing cabinet having a built in, three-position, dial-type combination lock; or a steel filing cabinet equipped with a steel lock bar, provided it is secured by a GSA approved changeable combination padlock.

11a

E. *Combinations.* Combinations to security equipment and devices shall be changed only by persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination is transferred from the office to which the equipment is assigned, whenever a combination has been subjected to possible compromise, and at least once every year. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest category of classified information or material authorized for storage in the security equipment concerned.

F. *Telecommunications Conversations.* Classified information shall not be revealed in telecommunications conversations, except as may be authorized under Appendix B with respect to the transmission of classified information over approved communications circuits or systems.

G. *Responsibilities of Custodians.* Custodians of classified material shall be responsible for providing protection and accountability for such material at all times and particularly for locking classified material in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified information or material by sight or sound, and classified information shall not be discussed with or in the presence of unauthorized persons.

APPENDIX B

TRANSMISSION OF CLASSIFIED INFORMATION

A. *Preparation and Receipting.* Classified information and material shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and address. The outer cover shall be sealed and addressed with no indication of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential material shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be signed by the recipient and returned to the sender.

B. *Transmission of Top Secret.* The transmission of Top Secret information and material shall be effected preferably by oral discussions in person between the officials concerned. Otherwise the transmission of Top Secret information and material shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for that purpose, over authorized communications circuits in encrypted form or by other means authorized by the National Security Council; except that in the case of information transmitted by the Federal Bureau of Investigation, such means of transmission may be used as are approved by the Director, Federal Bureau of Investigation, unless express reservation to the contrary is made in exceptional cases by the originating Department.

C. *Transmission of Secret.* The transmission of Secret material shall be effected in the following manner.

(1) *The Fifty States, District of Columbia, Puerto Rico.* Secret information and material may be transmitted within and between the forty-eight contiguous states and District of Columbia, or wholly within the State of Hawaii, the State of Alaska, or the Commonwealth of Puerto Rico by one of the means authorized for Top Secret information and material, the United States Postal Service registered mail and protective services provided by the United States air or surface commercial carriers under such conditions as may be prescribed by the head of the Department concerned.

(2) *Other Areas, Vessels, Military Postal Services, Aircraft.* Secret information and material may be transmitted from or to or within areas other than those specified in (1) above, by one of the means established for Top Secret information and material, captains or masters of vessels of United States registry under contract to a Department of the Executive Branch, United States registered mail through Army, Navy or Air Force Postal Service facilities provided that material does not at any time pass out of United States citizen control and does not pass through a foreign postal system, and commercial aircraft under charter to the United States and military or other government aircraft.

(3) *Canadian Government Installations.* Secret information and material may be transmitted between United States Government or Canadian Government installations, or both, in the forty-eight contiguous states, Alaska, the District of Columbia and Canada by United States and Canadian registered mail with registered mail receipt.

(4) *Special Cases.* Each Department may authorize the use of the United States Postal Service registered mail outside the forty-eight contiguous states, the District of Columbia, the State of Hawaii, the State of Alaska, and the Commonwealth of Puerto Rico if warranted by security conditions and essential operational requirements provided that the material does not at any time pass out of United States Government and United States citizen control and does not pass through a foreign postal system.

12a

D. *Transmittal of Confidential.* Confidential information and material shall be transmitted within the forty-eight contiguous states and the District of Columbia, or wholly within Alaska, Hawaii, the Commonwealth of Puerto Rico, or a United States possession, by one of the means established for higher classifications, or by certified or first class mail. Outside these areas, Confidential information and material shall be transmitted in the same manner as authorized for higher classifications.

E. *Alternative Transmission of Confidential.* Each Department having authority to classify information or material as "Confidential" may issue regulations authorizing alternative or additional methods for the transmission of material classified "Confidential" outside of the Department. In the case of material originated by another agency, the method of transmission must be at least as secure as the transmission procedures imposed by the originator.

F. *Transmission Within a Department.* Department regulations governing the preparation and transmission of classified information within a Department shall ensure a degree of security equivalent to that prescribed above for transmission outside the Department.

[FR Doc.72-7713 Filed 5-17-72;5:04 pm]

13a

Title 3—The President

EXECUTIVE ORDER 11652

Classification and Declassification of National Security Information and Material

The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch.

Within the Federal Government there is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our allies. To protect against actions hostile to the United States, of both an overt and covert nature, it is essential that such official information and material be given only limited dissemination.

This official information or material, referred to as classified information or material in this order, is expressly exempted from public disclosure by Section 552(b)(1) of Title 5, United States Code. Wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution.

To ensure that such information and material is protected, but only to the extent and for such period as is necessary, this order identifies the information to be protected, prescribes classification, downgrading, declassification and safeguarding procedures to be followed, and establishes a monitoring system to ensure its effectiveness.

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, it is hereby ordered:

SECTION 1. *Security Classification Categories.* Official information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (hereinafter collectively termed "national security") shall be classified in one of three categories, namely "Top Secret," "Secret," or "Confidential," depending upon the degree of its significance to national security. No other categories shall be used to identify official information or material as requiring protection in the interest of national security, except as otherwise expressly provided by statute. These classification categories are defined as follows:

(A) *"Top Secret."* "Top Secret" refers to that national security information or material which requires the highest degree of protection. The test for assigning "Top Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the

11a

national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with the utmost restraint.

(B) *"Secret."* "Secret" refers to that national security information or material which requires a substantial degree of protection. The test for assigning "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. The classification "Secret" shall be sparingly used.

(C) *"Confidential."* "Confidential" refers to that national security information or material which requires protection. The test for assigning "Confidential" classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

SEC. 2. *Authority to Classify.* The authority to originally classify information or material under this order shall be restricted solely to those offices within the executive branch which are concerned with matters of national security, and shall be limited to the minimum number absolutely required for efficient administration. Except as the context may otherwise indicate, the term "Department" as used in this order shall include agency or other governmental unit.

(A) The authority to originally classify information or material under this order as "Top Secret" shall be exercised only by such officials as the President may designate in writing and by:

(1) The heads of the Departments listed below;

(2) Such of their senior principal deputies and assistants as the heads of such Departments may designate in writing; and

(3) Such heads and senior principal deputies and assistants of major elements of such Departments, as the heads of such Departments may designate in writing.

Such offices in the Executive Office of the President as the President may designate in writing
Central Intelligence Agency
Atomic Energy Commission
Department of State
Department of the Treasury
Department of Defense
Department of the Army
Department of the Navy
Department of the Air Force
United States Arms Control and Disarmament Agency

Department of Justice
National Aeronautics and Space Administration
Agency for International Development

(B) The authority to originally classify information or material under this order as "Secret" shall be exercised only by:

(1) Officials who have "Top Secret" classification authority;

(2) Such subordinates as officials with "Top Secret" classification authority under (A) (1) and (2) above may designate in writing; and

(3) The heads of the following named Departments and such senior principal deputies or assistants as they may designate in writing.

Department of Transportation
Federal Communications Commission
Export-Import Bank of the United States
Department of Commerce
United States Civil Service Commission
United States Information Agency
General Services Administration
Department of Health, Education, and Welfare
Civil Aeronautics Board
Federal Maritime Commission
Federal Power Commission
National Science Foundation
Overseas Private Investment Corporation

(C) The authority to originally classify information or material under this order as "Confidential" may be exercised by officials who have "Top Secret" or "Secret" classification authority and such officials as they may designate in writing.

(D) Any Department not referred to herein and any Department or unit established hereafter shall not have authority to originally classify information or material under this order, unless specifically authorized hereafter by an Executive order.

SEC. 3. *Authority to Downgrade and Declassify.* The authority to downgrade and declassify national security information or material shall be exercised as follows:

(A) Information or material may be downgraded or declassified by the official authorizing the original classification, by a successor in capacity or by a supervisory official of either.

(B) Downgrading and declassification authority may also be exercised by an official specifically authorized under regulations issued by the head of the Department listed in Sections 2(A) or (B) hereof.

(C) In the case of classified information or material officially transferred by or pursuant to statute or Executive order in conjunction with a transfer of function and not merely for storage purposes, the receiving Department shall be deemed to be the originating Department for all purposes under this order including downgrading and declassification.

16a

(D) In the case of classified information or material not officially transferred within (C) above, but originated in a Department which has since ceased to exist, each Department in possession shall be deemed to be the originating Department for all purposes under this order. Such information or material may be downgraded and declassified by the Department in possession after consulting with any other Departments having an interest in the subject matter.

(E) Classified information or material transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded and declassified by the Archivist of the United States in accordance with this order, directives of the President issued through the National Security Council and pertinent regulations of the Departments.

(F) Classified information or material with special markings, as described in Section 8, shall be downgraded and declassified as required by law and governing regulations.

SEC. 4. *Classification.* Each person possessing classifying authority shall be held accountable for the propriety of the classifications attributed to him. Both unnecessary classification and over-classification shall be avoided. Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security. The following rules shall apply to classification of information under this order:

(A) *Documents in General.* Each classified document shall show on its face its classification and whether it is subject to or exempt from the General Declassification Schedule. It shall also show the office of origin, the date of preparation and classification and, to the extent practicable, be so marked as to indicate which portions are classified, at what level, and which portions are not classified in order to facilitate excerpting and other use. Material containing references to classified materials, which references do not reveal classified information, shall not be classified.

(B) *Identification of Classifying Authority.* Unless the Department involved shall have provided some other method of identifying the individual at the highest level that authorized classification in each case, material classified under this order shall indicate on its face the identity of the highest authority authorizing the classification. Where the individual who signs or otherwise authenticates a document or item has also authorized the classification, no further annotation as to his identity is required.

(C) *Information or Material Furnished by a Foreign Government or International Organization.* Classified information or material furnished to the United States by a foreign government or international organization shall either retain its original classification or be assigned a United States classification. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information or material.

(D) *Classification Responsibilities.* A holder of classified information or material shall observe and respect the classification assigned by the originator. If a holder believes that there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification under this order, he shall so inform the originator who shall thereupon re-examine the classification.

SEC. 5. *Declassification and Downgrading.* Classified information and material, unless declassified earlier by the original classifying authority, shall be declassified and downgraded in accordance with the following rules:

(A) *General Declassification Schedule.* (1) *"Top Secret."* Information or material originally classified "Top Secret" shall become automatically downgraded to "Secret" at the end of the second full calendar year following the year in which it was originated, downgraded to "Confidential" at the end of the fourth full calendar year following the year in which it was originated, and declassified at the end of the tenth full calendar year following the year in which it was originated.

(2) *"Secret."* Information and material originally classified "Secret" shall become automatically downgraded to "Confidential" at the end of the second full calendar year following the year in which it was originated, and declassified at the end of the eighth full calendar year following the year in which it was originated.

(3) *"Confidential."* Information and material originally classified "Confidential" shall become automatically declassified at the end of the sixth full calendar year following the year in which it was originated.

(B) *Exemptions from General Declassification Schedule.* Certain classified information or material may warrant some degree of protection for a period exceeding that provided in the General Declassification Schedule. An official authorized to originally classify information or material "Top Secret" may exempt from the General Declassification Schedule any level of classified information or material originated by him or under his supervision if it falls within one of the categories described below. In each case such official shall specify in writing on the material the exemption category being claimed and, unless impossible, a date or event for automatic declassification. The use of the exemption authority shall be kept to the absolute minimum consistent with national security requirements and shall be restricted to the following categories:

(1) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.

(2) Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

(3) Classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security.

(4) Classified information or material the disclosure of which would place a person in immediate jeopardy.

(C) *Mandatory Review of Exempted Material.* All classified information and material originated after the effective date of this order which is exempted under (B) above from the General Declassification Schedule shall be subject to a classification review by the originating Department at any time after the expiration of ten years from the date of origin provided:

(1) A Department or member of the public requests a review;

(2) The request describes the record with sufficient particularity to enable the Department to identify it; and

(3) The record can be obtained with only a reasonable amount of effort.

Information or material which no longer qualifies for exemption under (B) above shall be declassified. Information or material continuing to qualify under (B) shall be so marked and, unless impossible, a date for automatic declassification shall be set.

(D) *Applicability of the General Declassification Schedule to Previously Classified Material.* Information or material classified before the effective date of this order and which is assigned to Group 4 under Executive Order No. 10501, as amended by Executive Order No. 10964, shall be subject to the General Declassification Schedule. All other information or material classified before the effective date of this order, whether or not assigned to Groups 1, 2, or 3 of Executive Order No. 10501, as amended, shall be excluded from the General Declassification Schedule. However, at any time after the expiration of ten years from the date of origin it shall be subject to a mandatory classification review and disposition under the same conditions and criteria that apply to classified information and material created after the effective date of this order as set forth in (B) and (C) above.

(E) *Declassification of Classified Information or Material After Thirty Years.* All classified information or material which is thirty years old or more, whether originating before or after the effective date of this order, shall be declassified under the following conditions:

(1) All information and material classified after the effective date of this order shall, whether or not declassification has been requested, become automatically declassified at the end of thirty full calendar years after the date of its original classification except for such specifically identified information or material which the head of the originating Department personally determines in writing at that time to require continued protection because such continued protection is essential to the national security or disclosure would place a person in immediate jeopardy. In such case, the head of the Department shall also specify the period of continued classification.

(2) All information and material classified before the effective date of this order and more than thirty years old shall be systematically reviewed for declassification by the Archivist of the United States by the end of the thirtieth full calendar year following the year in which it was

19a

originated. In his review, the Archivist will separate and keep protected only such information or material as is specifically identified by the head of the Department in accordance with (E)(1) above. In such case, the head of the Department shall also specify the period of continued classification.

(F) *Departments Which Do Not Have Authority For Original Classification.* The provisions of this section relating to the declassification of national security information or material shall apply to Departments which, under the terms of this order, do not have current authority to originally classify information or material, but which formerly had such authority under previous Executive orders.

SEC. 6. *Policy Directives on Access, Marking, Safekeeping, Accountability, Transmission, Disposition and Destruction of Classified Information and Material.* The President acting through the National Security Council shall issue directives which shall be binding on all Departments to protect classified information from loss or compromise. Such directives shall conform to the following policies:

(A) No person shall be given access to classified information or material unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of his duties.

(B) All classified information and material shall be appropriately and conspicuously marked to put all persons on clear notice of its classified contents.

(C) Classified information and material shall be used, possessed, and stored only under conditions which will prevent access by unauthorized persons or dissemination to unauthorized persons.

(D) All classified information and material disseminated outside the executive branch under Executive Order No. 10865 or otherwise shall be properly protected.

(E) Appropriate accountability records for classified information shall be established and maintained and such information and material shall be protected adequately during all transmissions.

(F) Classified information and material no longer needed in current working files or for reference or record purposes shall be destroyed or disposed of in accordance with the records disposal provisions contained in Chapter 33 of Title 44 of the United States Code and other applicable statutes.

(G) Classified information or material shall be reviewed on a systematic basis for the purpose of accomplishing downgrading, declassification, transfer, retirement and destruction at the earliest practicable date.

SEC. 7. *Implementation and Review Responsibilities.* (A) The National Security Council shall monitor the implementation of this order. To assist the National Security Council, an Interagency Classification Review Committee shall be established, composed of representatives of the Departments of State, Defense and Justice, the Atomic Energy Commission, the Central Intelligence Agency and the National

Security Council Staff and a Chairman designated by the President. Representatives of other Departments in the executive branch may be invited to meet with the Committee on matters of particular interest to those Departments. This Committee shall meet regularly and on a continuing basis shall review and take action to ensure compliance with this order, and in particular:

(1) The Committee shall oversee Department actions to ensure compliance with the provisions of this order and implementing directives issued by the President through the National Security Council.

(2) The Committee shall, subject to procedures to be established by it, receive, consider and take action on suggestions and complaints from persons within or without the government with respect to the administration of this order, and in consultation with the affected Department or Departments assure that appropriate action is taken on such suggestions and complaints.

(3) Upon request of the Committee Chairman, any Department shall furnish to the Committee any particular information or material needed by the Committee in carrying out its functions.

(B) To promote the basic purposes of this order, the head of each Department originating or handling classified information or material shall:

(1) Prior to the effective date of this order submit to the Interagency Classification Review Committee for approval a copy of the regulations it proposes to adopt pursuant to this order.

(2) Designate a senior member of his staff who shall ensure effective compliance with and implementation of this order and shall also chair a Departmental committee which shall have authority to act on all suggestions and complaints with respect to the Department's administration of this order.

(3) Undertake an initial program to familiarize the employees of his Department with the provisions of this order. He shall also establish and maintain active training and orientation programs for employees concerned with classified information or material. Such programs shall include, as a minimum, the briefing of new employees and periodic reorientation during employment to impress upon each individual his responsibility for exercising vigilance and care in complying with the provisions of this order. Additionally, upon termination of employment or contemplated temporary separation for a sixty-day period or more, employees shall be debriefed and each reminded of the provisions of the Criminal Code and other applicable provisions of law relating to penalties for unauthorized disclosure.

(C) The Attorney General, upon request of the head of a Department, his duly designated representative, or the Chairman of the above described Committee, shall personally or through authorized representatives of the Department of Justice render an interpretation of this order with respect to any question arising in the course of its administration.

2/2

SEC. 8. *Material Covered by the Atomic Energy Act.* Nothing in this order shall supersede any requirements made by or under the Atomic Energy Act of August 30, 1954, as amended. "Restricted Data," and material designated as "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 the regulations of the Atomic Energy Commission.

SEC. 9. *Special Departmental Arrangements.* The originating Department or other appropriate authority may impose, in conformity with the provisions of this order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography.

SEC. 10. *Exceptional Cases.* In an exceptional case when a person or Department not authorized to classify information originates information which is believed to require classification, such person or Department shall protect that information in the manner prescribed by this order. Such persons or Department shall transmit the information forthwith, under appropriate safeguards, to the Department having primary interest in the subject matter with a request that a determination be made as to classification.

SEC. 11. *Declassification of Presidential Papers.* The Archivist of the United States shall have authority to review and declassify information and material which has been classified by a President, his White House Staff or special committee or commission appointed by him and which the Archivist has in his custody at any archival depository, including a Presidential Library. Such declassification shall only be undertaken in accord with: (i) the terms of the donor's deed of gift, (ii) consultations with the Departments having a primary subject-matter interest, and (iii) the provisions of Section 5.

SEC. 12. *Historical Research and Access by Former Government Officials.* The requirement in Section 6(A) that access to classified information or material be granted only as is necessary for the performance of one's duties shall not apply to persons outside the executive branch who are engaged in historical research projects or who have previously occupied policy-making positions to which they were appointed by the President; *Provided,* however, that in each case the head of the originating Department shall:

(i) determine that access is clearly consistent with the interests of national security; and

(ii) take appropriate steps to assure that classified information or material is not published or otherwise compromised.

Access granted a person by reason of his having previously occupied a policy-making position shall be limited to those papers which the former official originated, reviewed, signed or received while in public office.

SEC. 13. *Administrative and Judicial Action.* (A) Any officer or employee of the United States who unnecessarily classifies or over-

classifies information or material shall be notified that his actions are in violation of the terms of this order or of a directive of the President issued through the National Security Council. Repeated abuse of the classification process shall be grounds for an administrative reprimand. In any case where the Departmental committee or the Interagency Classification Review Committee finds that unnecessary classification or overclassification has occurred, it shall make a report to the head of the Department concerned in order that corrective steps may be taken.

(B) The head of each Department is directed to take prompt and stringent administrative action against any officer or employee of the United States, at any level of employment, determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by or under this order or a directive of the President issued through the National Security Council. Where a violation of criminal statutes may be involved, Departments will refer any such case promptly to the Department of Justice.

SEC. 14. *Revocation of Executive Order No. 10501.* Executive Order No. 10501 of November 5, 1953, as amended by Executive Orders No. 10816 of May 8, 1959, No. 10901 of January 11, 1961, No. 10964 of September 20, 1961, No. 10985 of January 15, 1962, No. 11097 of March 6, 1963 and by Section 1(a) of No. 11382 of November 28, 1967, is superseded as of the effective date of this order.

SEC. 15. *Effective date.* This order shall become effective on June 1, 1972.

Richard Nixon

THE WHITE HOUSE,
March 8, 1972.

[FR Doc.72-3782 Filed 3-9-72; 11:01 am]

Executive Order 12065 June 28, 1978

National Security Information

By the authority vested in me as President by the Constitution and laws of the United States of America, in order to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure, it is hereby ordered as follows:

TABLE OF CONTENTS

24a

SECTION 1. ORIGINAL CLASSIFICATION.

1-1. *Classification Designation.*

1-101. Except as provided in the Atomic Energy Act of 1954, as amended, this Order provides the only basis for classifying information. Information may be classified in one of the three designations listed below. If there is reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive designation should be used, or the information should not be classified.

1-102. "Top Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

1-103. "Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

1-104. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security.

1-2. *Classification Authority.*

1-201. *Top Secret.* Authority for original classification of information as Top Secret may be exercised only by the President, by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, and by officials to whom such authority is delegated in accordance with Section 1-204:

The Secretary of State

The Secretary of the Treasury

The Secretary of Defense

The Secretary of the Army

The Secretary of the Navy

The Secretary of the Air Force

The Attorney General

The Secretary of Energy

The Chairman, Nuclear Regulatory Commission

The Director, Arms Control and Disarmament Agency

The Director of Central Intelligence

The Administrator, National Aeronautics and Space Administration

The Administrator of General Services (delegable only to the Director, Federal Preparedness Agency and to the Director, Information Security Oversight Office)

1-202. *Secret.* Authority for original classification of information as Secret may be exercised only by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, by officials who have Top

25a

Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:

The Secretary of Commerce

The Secretary of Transportation

The Administrator, Agency for International Development

The Director, International Communication Agency

1-203. *Confidential.* Authority for original classification of information as Confidential may be exercised only by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, by officials who have Top Secret or Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:

The President and Chairman, Export-Import Bank of the United States

The President and Chief Executive Officer, Overseas Private Investment Corporation

1-204. *Limitations on Delegation of Classification Authority.*

(a) Authority for original classification of information as Top Secret may be delegated only to principal subordinate officials who have a frequent need to exercise such authority as determined by the President or by agency heads listed in Section 1-201.

(b) Authority for original classification of information as Secret may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201 and 1-202, and by officials with Top Secret classification authority.

(c) Authority for original classification of information as Confidential may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201, 1-202, and 1-203, and by officials with Top Secret classification authority.

(d) Delegated original classification authority may not be redelegated.

(e) Each delegation of original classification authority shall be in writing by name or title of position held.

(f) Delegations of original classification authority shall be held to an absolute minimum. Periodic reviews of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

1-205. *Exceptional Cases.* When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be protected in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority. That agency shall decide within 30 days whether to classify that information. If it is not clear which agency should get the information, it shall be sent to the Director of the Information Security Oversight Office established in Section 5-2 for a determination.

26a

1-3. *Classification Requirements.*

1-301. Information may not be considered for classification unless it concerns:

(a) military plans, weapons, or operations;

(b) foreign government information;

(c) intelligence activities, sources or methods;

(d) foreign relations or foreign activities of the United States;

(e) scientific, technological, or economic matters relating to the national security;

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

(g) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President, by a person designated by the President pursuant to Section 1-201, or by an agency head.

1-302. Even though information is determined to concern one or more of the criteria in Section 1-301, it may not be classified unless an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security.

1-303. Unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security.

1-304. Each determination under the criterion of Section 1-301(g) shall be reported promptly to the Director of the Information Security Oversight Office.

1-4. *Duration of Classification.*

1-401. Except as permitted in Section 1-402, at the time of the original classification each original classification authority shall set a date or event for automatic declassification no more than six years later.

1-402. Only officials with Top Secret classification authority and agency heads listed in Section 1-2 may classify information for more than six years from the date of the original classification. This authority shall be used sparingly. In such cases, a declassification date or event, or a date for review, shall be set. This date or event shall be as early as national security permits and shall be no more than twenty years after original classification, except that for foreign government information the date or event may be up to thirty years after original classification.

1-5. *Identification and Markings.*

1-501. At the time of original classification, the following shall be shown on the face of paper copies of all classified documents:

(a) the identity of the original classification authority;

(b) the office of origin;

(c) the date or event for declassification or review; and

(d) one of the three classification designations defined in Section 1-1.

27a

1-502. Documents classified for more than six years shall also be marked with the identity of the official who authorized the prolonged classification. Such documents shall be annotated with the reason the classification is expected to remain necessary, under the requirements of Section 1-3, despite the passage of time. The reason for the prolonged classification may be stated by reference to criteria set forth in agency implementing regulations. These criteria shall explain in narrative form the reason the information needs to be protected beyond six years. If the individual who signs or otherwise authenticates a document also is authorized to classify it, no further annotation of identity is required.

1-503. Only the designations prescribed by this Order may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" may not be used for that purpose. Terms such as "Conference" or "Agency" may not be used in conjunction with the classification designations prescribed by this Order; e.g., "Agency Confidential" or "Conference Confidential."

1-504. In order to facilitate excerpting and other uses, each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified. The Director of the Information Security Oversight Office may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information.

1-505. Foreign government information shall either retain its original classification designation or be assigned a United States classification designation that shall ensure a degree of protection equivalent to that required by the entity that furnished the information.

1-506. Classified documents that contain or reveal information that is subject to special dissemination and reproduction limitations authorized by this Order shall be marked clearly so as to place the user on notice of the restrictions.

1-6. *Prohibitions.*

1-601. Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

1-602. Basic scientific research information not clearly related to the national security may not be classified.

1-603. A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Order until and unless the government acquires a proprietary interest in the product. This Order does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188).

1-604. References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.

1-605. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Order or to prevent or delay the public release of such information.

1-606. No document originated on or after the effective date of this Order may be classified after an agency has received a request for the document under the

28a

Freedom of Information Act or the Mandatory Review provisions of this Order (Section 3-5), unless such classification is consistent with this Order and is authorized by the agency head or deputy agency head. Documents originated before the effective date of this Order and subject to such a request may not be classified unless such classification is consistent with this Order and is authorized by the senior official designated to oversee the agency information security program or by an official with Top Secret classification authority. Classification authority under this provision shall be exercised personally, on a document-by-document basis.

1-607. Classification may not be restored to documents already declassified and released to the public under this Order or prior Orders.

SECTION 2. DERIVATIVE CLASSIFICATION.

2-1. *Use of Derivative Classification.*

2-101. Original classification authority shall not be delegated to 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.

2-102. Persons who apply such derivative classification markings shall:

(a) respect original classification decisions;

(b) verify the information's current level of classification so far as practicable before applying the markings; and

(c) carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings, in accordance with Sections 2-2 and 2-301 below. A single marking may be used for documents based on multiple sources.

2-2. *Classification Guides.*

2-201. Classification guides used to direct derivative classification shall specifically identify the information to be classified. Each classification guide shall specifically indicate how the designations, time limits, markings, and other requirements of this Order are to be applied to the information.

2-202. Each such guide shall be approved personally and in writing by an agency head listed in Section 1-2 or by an official with Top Secret classification authority. Such approval constitutes an original classification decision.

2-3. *New Material.*

2-301. New material that derives its classification from information classified on or after the effective date of this Order shall be marked with the declassification date or event, or the date for review, assigned to the source information.

2-302. New material that derives its classification from information classified under prior Orders shall be treated as follows:

(a) If the source material bears a declassification date or event twenty years or less from the date or origin, that date or event shall be carried forward on the new material.

(b) If the source material bears no declassification date or event or is marked for declassification beyond twenty years, the new material shall be marked with a

40-002 O—79——14

date for review for declassification at twenty years from the date of original classification of the source material.

(c) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond thirty years, the new material shall be marked for review for declassification at thirty years from the date of original classification of the source material.

SECTION 3. DECLASSIFICATION AND DOWNGRADING.

3-1. *Declassification Authority.*

3-101. The authority to declassify or downgrade information classified under this or prior Orders shall be exercised only as specified in Section 3-1.

3-102. Classified information may be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, by a successor, or by a supervisory official of either.

3-103. Agency heads named in Section 1-2 shall designate additional officials at the lowest practicable echelons to exercise declassification and downgrading authority.

3-104. 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 until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.

3-105. The provisions of this Order relating to declassification shall also apply to agencies which, under the terms of this Order, do not have original classification authority but which had such authority under prior Orders.

3-2. *Transferred Information.*

3-201. For classified information transferred in conjunction with a transfer of functions—not merely for storage purposes—the receiving agency shall be deemed to be the originating agency for all purposes under this Order.

3-202. For classified information not transferred in accordance with Section 3-201, but originated in an agency which has ceased to exist, each agency in possession shall be deemed to be the originating agency for all purposes under this Order. Such information may be declassified or downgraded by the agency in possession after consulting with any other agency having an interest in the subject matter.

3-203. Classified information transferred to the General Services Administration for accession into the Archives of the United States 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 the agency guidelines.

3-204. After the termination of a Presidential administration, the Archivist of the United States shall review and declassify or downgrade all information classified by the President, the White House Staff, committees or commissions appointed by the President, or others acting on the President's behalf. Such declassification shall only be undertaken in accordance with the provisions of Section 3-504.

30a

3-3. *Declassification Policy.*

3-301. Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event.

3-302. When information is reviewed for declassification pursuant to this Order or the Freedom of Information Act, it shall be declassified unless the declassification authority established pursuant to Section 3-1 determines that the information continues to meet the classification requirements prescribed in Section 1-3 despite the passage of time.

3-303. 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.

3-4. *Systematic Review for Declassification.*

3-401. Classified information constituting permanently valuable records of the Government, as defined by 44 U.S.C. 2103, and information in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be reviewed for declassification as it becomes twenty years old. Agency heads listed in Section 1-2 and officials designated by the President pursuant to Section 1-201 of this Order may extend classification beyond twenty years, but only in accordance with Sections 3-3 and 3-402. This authority may not be delegated. When classification is extended beyond twenty years, a date no more than ten years later shall be set for declassification or for the next review. That date shall be marked on the document. Subsequent reviews for declassification shall be set at no more than ten year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of documents or information.

3-402. Within 180 days after the effective date of this Order, the agency heads listed in Section 1-2 and the heads of agencies which had original classification authority under prior orders shall, after consultation with the Archivist of the United States and review by the Information Security Oversight Office, issue and maintain guidelines for systematic review covering twenty-year old classified information under their jurisdiction. These guidelines shall state specific, limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond twenty years is needed. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of

the issuing authority, be used by any agency having custody of the information. All information not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of twenty years from the date of original classification.

3–403. Nothwithstanding Sections 3–401 and 3–402, the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review and declassification of classified information concerning the identities of clandestine human agents. These procedures shall be consistent, so far as practicable, with the objectives of Sections 3–401 and 3–402. Prior to implementation, they shall be reviewed and approved by the Director of the Information Security Oversight Office and, with respect to matters pertaining to intelligence sources and methods, by the director of Central Intelligence. Disapproval of procedures by the Director of the Information Security Oversight Office may be appealed to the National Security Council. In such cases, the procedures shall not be implemented until the appeal is decided.

3–404. Foreign government information shall be exempt from automatic declassification and twenty year systematic review. Unless declassified earlier, such information shall be reviewed for declassification thirty years from its date of origin. Such review shall be in accordance with the provisions of Section 3–3 and with guidelines developed by agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information.

3–405. Transition to systematic review at twenty years shall be implemented as rapidly as practicable and shall be completed no more than ten years from the effective date of this Order.

3–5. *Mandatory Review for Declassification.*

3–501. Agencies shall establish a mandatory review procedure to handle requests by a member of the public, by a government employee, or by an agency, to declassify and release information. This procedure shall apply to information classified under this Order or prior Orders. Except as provided in Section 3–503, upon such a request the information shall be reviewed for possible declassification, provided the request reasonably describes the information. Requests for declassification under this provision shall be acted upon within 60 days. After review, the information or any reasonably segregable portion thereof that no longer requires protection under this Order shall be declassified and released unless withholding is otherwise warranted under applicable law.

3–502. Requests for declassification which are submitted under the provisions of the Freedom of Information Act shall be processed in accordance with the provisions of that Act.

3–503. Information less than ten years old which was originated by the President, by the White House Staff, or by committees or commissions appointed by the President, or by others acting on behalf of the President, including such information in the possession and control of the Administrator of General Services pursuant to

32a

44 U.S.C. 2107 or 2107 note, is exempted from the provisions of Section 3-501. Such information over ten years old shall be subject to mandatory review for declassification. Requests for mandatory review shall be processed in accordance with procedures developed by the Archivist of the United States. These procedures shall provide for consultation with agencies having primary subject matter interest. Any decision by the Archivist may be appealed to the director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council through the process set forth in Section 3-104.

3-504. Requests for declassification of classified documents originated by an agency but in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be referred by the Archivist to the agency of origin for processing in accordance with Section 3-501 and for direct response to the requestor. The Archivist shall inform requestors of such referrals.

3-505. No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act or this Order's Mandatory Review provision, refuse to confirm the existence or non-existence of the document, unless the fact of its existence or non-existence would itself be classifiable under this Order.

3-6. *Downgrading.*

3-601. Classified information that is marked for automatic downgrading is downgraded accordingly without notification to holders.

3-602. Classified information that is not marked for automatic downgrading may be assigned a lower classification designation by the originator or by other authorized officials when such downgrading is appropriate. Notice of downgrading shall be provided to holders of the information to the extent practicable.

SECTION 4. SAFEGUARDING.

4-1. *General Restrictions on Access.*

4-101. No person may be given access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties.

4-102. All classified information shall be marked conspicuously to put users on notice of its current classification status and, if appropriate, to show any special distribution or reproduction restrictions authorized by this Order.

4-103. Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, and transmitted only under conditions that will provide adequate protection and prevent access by unauthorized persons.

4-104. Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of Chapters 21 and 33 of Title 44 of the United States Code, which governs disposition of Federal records.

4-105. Classified information disseminated outside the Executive branch shall be given protection equivalent to that afforded within the Executive branch.

4–2. *Special Access Programs.*

4–201. Agency heads listed in Section 1–201 may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or prior Orders. Such programs may be created or continued only by written direction and only by those agency heads and, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Classified information in such programs shall be declassified according to the provisions of Section 3.

4–202. Special access programs may be created or continued only on a specific showing that:

(a) normal management and safeguarding procedures are not sufficient to limit need-to-know or access;

(b) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and

(c) the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

4–203. All special access programs shall be reviewed regularly and, except those required by treaty or international agreement, shall terminate automatically every five years unless renewed in accordance with the procedures in Section 4–2.

4–204. Within 180 days after the effective date of this Order, agency heads shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in Section 4–2. Each of those agency heads shall also establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office shall have non-delegable access to all such accountings.

4–3. *Access by Historical Researchers and Former Presidential Appointees.*

4–301. The requirement in Section 4–101 that access to classified information may be granted only as is necessary for the performance of official duties may be waived as provided in Section 4–302 for persons who:

(a) are engaged in historical research projects, or

(b) previously have occupied policy-making positions to which they were appointed by the President.

4–302. Waivers under Section 4–301 may be granted only if the agency with jurisdiction over the information:

(a) makes a written determination that access is consistent with the interests of national security;

(b) takes appropriate steps to ensure that access is limited to specific categories of information over which that agency has classification jurisdiction;

(c) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed or received while serving as a Presidential appointee.

34a

4–4. *Reproduction Controls.*

4–401. Top Secret documents may not be reproduced without the consent of the originating agency unless otherwise marked by the originating office.

4–402. Reproduction of Secret and Confidential documents may be restricted by the originating agency.

4–403. Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.

4–404. Records shall be maintained by all agencies that reproduce paper copies of classified documents to show the number and distribution of reproduced copies of all Top Secret documents, of all documents covered by special access programs distributed outside the originating agency, and of all Secret and all Confidential documents which are marked with special dissemination and reproduction limitations in accordance with Section 1–506.

4–405. Sections 4–401 and 4–402 shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However, such reproduced documents that remain classified after review must be destroyed after they are used.

SECTION 5. IMPLEMENTATION AND REVIEW.

5–1. *Oversight.*

5–101. The National Security Council may review all matters with respect to the implementation of this Order and shall provide overall policy direction for the information security program.

5–102. The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. This responsibility shall be delegated to an Information Security Oversight Office.

5–2. *Information Security Oversight Office.*

5–201. The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Administrator also shall have authority to appoint a staff for the Office.

5–202. The Director shall:

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

(b) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program, including appeals from decisions on declassification requests pursuant to Section 3–503;

(c) exercise the authority to declassify information provided by Sections 3–104 and 3–503;

(d) 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;

(e) report annually to the President through the Administrator of General Services and the National Security Council on the implementation of this Order;

(f) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.

(g) exercise case-by-case classification authority in accordance with Section 1-205 and review requests for original classification authority from agencies or officials not granted original classification authority under Section 1-2 of this Order; and

(h) have the authority to conduct on-site reviews of the information security program of each agency that handles classified information and to require of each agency such reports, information, and other cooperation as necessary to fulfill his responsibilities. If such reports, inspection, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect until the appeal is decided or until one year from the date of the denial, whichever occurs first.

5-3. *Interagency Information Security Committee.*

5-301. There is established an Interagency Information Security Committee which shall be chaired by the Director and shall be comprised of representatives of the Secretaries of State, Defense, Treasury, and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council, the Domestic Policy Staff, and the Archivist of the United States.

5-302. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies.

5-303. The Committee shall meet at the call of the Chairman or at the request of a member agency and shall advise the Chairman on implementation of this order.

5-4. *General Responsibilities.*

5-401. A copy of any information security regulation and a copy of any guideline for systematic declassification review which has been adopted pursuant to this Order or implementing directives, shall be submitted to the Information Security Oversight Office. To the extent practicable, such regulations and guidelines should be unclassified.

5-402. Unclassified regulations that establish agency information security policy and unclassified guidelines for systematic declassification review shall be published in the FEDERAL REGISTER.

5-403. Agencies with original classification authority shall promulgate guides for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of this Order.

5-404. Agencies which originate or handle classified information shall:

36a

(a) designate a senior agency official to conduct an active oversight program to ensure effective implementation of this Order;

(b) designate a senior agency official to chair an agency committee with authority to act on all suggestions and complaints with respect to the agency's administration of the information security program;

(c) establish a process to decide appeals from denials of declassification requests submitted pursuant to Section 3-5;

(d) establish a program to familiarize agency and other personnel who have access to classified information with the provisions of this Order and implementing directives. This program shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order. The program shall encourage agency personnel to challenge, through Mandatory Review and other appropriate procedures, those classification decisions they believe to be improper;

(e) promulgate guidelines for systematic review in accordance with Section 3-402;

(f) establish procedures to prevent unnecessary access to classified information, including procedures which require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and which ensures that the number of people granted access to classified information is reduced to and maintained at the minimum number that is consistent with operational requirements and needs; and

(g) ensure that practices for safeguarding information are systematically reviewed and that those which are duplicative or unnecessary are eliminated.

5-405. Agencies shall submit to the Information Security Oversight Office such information or reports as the Director of the Office may find necessary to carry out the Office's responsibilities.

5-5. *Administrative Sanctions.*

5-501. If the Information Security Oversight Office finds that a violation of this Order or any implementing directives may have occurred, it shall make a report to the head of the agency concerned so that corrective steps may be taken.

5-502. Officers and employees of the United States Government shall be subject to appropriate administrative sanctions if they:

(a) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directives; or

(b) knowingly, willfully and without authorization disclose information properly classified under this Order or prior Orders or compromise properly classified information through negligence; or

(c) knowingly and willfully violate any other provision of this Order or implementing directive.

5-503. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations.

37a

5-504. Agency heads shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5-502 occurs. The Director of the Information Security Oversight Office shall be informed when such violations occur.

5-505. Agency heads shall report to the Attorney General evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.

SECTION 6. GENERAL PROVISIONS.

6-1. *Definitions.*

6-101. "Agency" has the meaning defined in 5 U.S.C. 552(e).

6-102. "Classified information" means information or material, herein collectively termed information, that is owned by, produced for or by, or under the control of, the United States Government, and that has been determined pursuant to this Order or prior Orders to require protection against unauthorized disclosure, and that is so designated.

6-103. "Foreign government information" means information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with, a foreign government or international organization of governments.

6-104. "National security" means the national defense and foreign relations of the United States.

6-105. "Declassification event" means an event which would eliminate the need for continued classification.

6-2. *General.*

6-201. Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and information designated as "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 pursuant thereto.

6-202. The Attorney General, upon request by the head of an agency, his duly designated representative, or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.

6-203. Executive Order No. 11652 of March 8, 1972, as amended by Executive Order No. 11714 of April 24, 1973, and as further amended by Executive Order No. 11862 of June 11, 1975, and the National Security Council Directive of May 17, 1972 (3 CFR 1085 (1971-75 Comp.)) are revoked.

6-204. This Order shall become effective on December 1, 1978, except that the functions of the Information Security Oversight Office specified in Sections 5-202(d) and 5-202(f) shall be effective immediately and shall be performed in the

38a

interim by the Interagency Classification Review Committee established pursuant to Executive Order No. 11652.

JIMMY CARTER

THE WHITE HOUSE,
June 28, 1978.

EDITORIAL NOTE: The President's statement of June 29, 1978, on issuing Executive Order 12065, is printed in the Weekly Compilation of Presidential Documents (vol. 14, p. 1193).

39 a