Exhibit A

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO

5510
Ser 092J/

~~TOP SECRET~~ - Unclassified upon removal of enclosure (1)

From: Director of Naval Intelligence (OP-092J)
To: U. S. Department of Justice, Internal Security Division

Subj: JONATHAN POLLARD SENTENCING AFFIDAVIT

Encl: (1) Court-Sealed, Original Weinberger Affidavit, OP-092 ~~TOP SECRET~~ Control Number 042-89

1. Enclosure (1) is the original TOP SECRET affidavit in aid of sentencing which former Secretary of Defense Caspar Weinberger presented to the trial court in the espionage prosecution of Jonathan Pollard. It is hereby temporarily transferred to your custody to assist the United States' response to a motion for reduction of sentence and/or related relief by Pollard. The Office of Naval Intelligence maintains no copies of this document.

2. You are requested to maintain this ~~TOP SECRET~~ document under an appropriate system of security controls. If it becomes necessary to reproduce enclosure (1), you are requested to provide the Office of Naval Intelligence (OP-092J) with information copies of the receipts or other control documents under which you transfer custody of any of those copies. It is further understood that enclosure (1) will be returned to the custody of the Office of Naval Intelligence as soon as practicable unless you are otherwise directed by the Trial Court or other competent judicial authority.

J. P. CALLAHAN
By direction

12-M-2766

~~TOP SECRET~~ UMBRA

GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE

WASHINGTON, D.C. 20301

January 7, 1987

MEMORANDUM FOR THE SECRETARY OF DEFENSE

SUBJECT: Sentencing Affidavit for Jonathan Pollard -- ACTION MEMORANDUM

Attached is an affidavit prepared for your signature. It is intended for use by the Court in assessing an appropriate sentence for Jonathan Pollard. The affidavit has been approved by CIA, DIA, NSA and Navy.

This document is lengthier than I would normally approve for your signature. The reason for the length is consistent with the scope of Pollard's espionage activities. Succinctly, he disclosed an incredible quantity of intelligence publications which encompassed a similarly broad scope and variety of intelligence information. Even so, only a handful from among the many thousands compromised are described herein. Those described are available for your review should you desire to do so.

It is the opinion of the intelligence agencies, and one which I share, that we must describe Pollard's activities with particularity. A lesser description of the damage he has done to the national security would risk an erroneous assumption by the sentencing judge that Pollard's disclosures to an ally have really done little to harm the United States. Of course, the probable consequence of such an assumption would be an inappropriate sentence. The factual descriptions of Pollard's activities contained in both the classified and unclassified sentencing memoranda which will be submitted by the U.S. Attorney are similarly lengthy.

This document will be handled in compartmented channels. Navy personnel will carry it to and from the judge, and one copy will be placed in the Department of Justice security vaults for review by defense counsel who have been properly cleared. The affidavit assumes that the Director of Naval Intelligence will provide permanent storage for it in his office.

I strongly recommend that you sign the affidavit.

H. Lawrence Garrett, III

Attachment

UNCLASSIFIED UPON REMOVAL
OF ATTACHMENT

~~TOP SECRET~~ UMBRA

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Criminal No. 86-0207
JONATHAN JAY POLLARD,	)	
defendant.	)	
	)	

DECLARATION OF THE SECRETARY OF DEFENSE

CASPAR W. WEINBERGER HEREBY DECLARES AND SAYS:

1. (U) I have been the Secretary of Defense and the chief executive officer of the Department of Defense (DOD), an executive department of the United States, 10 U.S.C. 131, since 20 January 1981. As Secretary of Defense, I have authority, direction and control over the DOD, 10 U.S.C. 133(b), and am a member of the National Security Council.

2. (U) As Secretary of Defense, I possess original classification authority for TOP SECRET information, including Sensitive Compartmented Information (SCI). SCI is information which derives from sources or methods which are especially vulnerable to unauthorized disclosures. That vulnerability may

stem from particularly fragile acquisition methodology, from sources especially susceptible to counter measures or deception techniques or even from danger to human life if the substantive information obtained is exposed. The fact that I possess this classification authority means that I am authorized to determine the significance and the proper classification of national security information, including TOP SECRET, SENSITIVE COMPARTMENTED INFORMATION (SCI), on behalf of the United States. The information I have prepared for the Court is submitted based upon my personal review of relevant information and my discussions with personnel who are knowledgeable about the data described herein.

3. (U) The information in this declaration is submitted for use by the Court as an aid in determining an appropriate sentence for the defendant, Jonathan Jay Pollard. It is my purpose to explain the nature and significance of the defendant's actions as I perceive them to have affected the security of the United States. I have detailed a considerable quantity of highly sensitive information, and therefore request that the Court review this document and deliver it under Court seal back into the hands of its bearer immediately upon completion of review. I also request that no one else be permitted to review this document unless it is necessary as a matter of law to do so, and then only if proper clearance and

access is ascertained. Should the document again be required by the Court, or by any Court with jurisdiction over this case, it will immediately be made available. I have directed that this document be retained by the Director of Naval Intelligence who will be responsible for its safekeeping and further delivery to the Court as required.

4. (U) I believe it is necessary to understand the purpose of intelligence acquisition before one can comprehend the significance of its loss. There are two primary reasons for gathering and analyzing intelligence information. The first, and most important in my view, is to gain the information required to direct U.S. resources as necessary to counter threats of external aggression. The second reason is to obtain the information necessary to efficiently and effectively direct the foreign policy of the United States. It necessarily follows that inappropriate disclosure of properly classified intelligence information intended to serve these purposes can be used to frustrate both the defensive and foreign policy goals of the United States, regardless of its recipient.

a. Intelligence information disclosed to a hostile foreign power can be used to produce counter measures, promote disinformation techniques, and even permit the more efficient and effective utilization of resources in manners inimical to

U.S. interests.

b. Unauthorized disclosures to friendly powers may cause as great a harm to the national security as to hostile powers because, once the information is removed from secure control systems, there is no enforceable requirement nor any incentive to provide effective controls for its safekeeping. Moreover, it is more probable than not that the information will be used for unintended purposes. Finally, such disclosures will tend to expose a larger picture of U.S. capabilities and knowledge, or lack thereof, than would be in the U.S. interest to reveal to another power, even to a friendly one.

5. (U) In this case, the defendant has admitted passing to his Israeli contacts an incredibly large quantity of classified information. At the outset I must state that the defendant's unlawful disclosures far exceed the limits of any official exchange of intelligence information with Israel. That being true, the damage to national security was complete the moment the information was given over. Ideally, I would detail for the Court all the information passed by the defendant to his Israeli contacts; unfortunately, the volume of data we know to have been passed is too great to permit that. Moreover, the defendant admits to having passed to his Israeli handlers a

quantity of documents great enough to occupy a space six feet by six feet by ten feet. I have chosen to present in three parts the data I consider significant. In the first part I have detailed the categories of information compromised and given brief but specific examples of actual documents passed. In the second part I explain the harm I perceive to have occurred, again with specific examples. In the third part I capsulize the overall significance of the defendant's activities.

PART ONE

CATEGORIES OF INFORMATION DISCLOSED

6. [redacted] Intelligence acquisitions [redacted]

It is known that the United States collects information on unfriendly nations, such as the Soviet Union, and it may be reasonably presumed that information is collected concerning other nations as well. What is not known is which nations, activities or enterprises are targets for intelligence collection, nor the depth of those collection activities.

[redacted]

25X1 and 6, E.O.13526

a. Ground Logistics Study - Saudi Arabia

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

7. [redacted] National Security Agency (NSA) information.

The National Security Agency is a component of the Department of Defense and is the U.S. agency responsible for intercepting foreign radio frequency signals and extracting

from those signals intelligence information known as signals intelligence (SIGINT). SIGINT includes sensitive details of foreign government political and military activities, and is used by the President and by senior government officials to protect the national security and to conduct foreign policy. As might be expected, such information is difficult to acquire and analyze, and is costly in terms of both time and money because of the technical complexity of radio and electronics communications and their susceptiblity to being disguised, encrypted and transmitted within precise and discrete communications channels.

a. That the National Security Agency collects intelligence through the intercept of foreign communications is well known,

25X1, 3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

25X1, 3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

b. NSA has developed a system for cataloguing radio frequency signals in order to enable it to recognize, intercept, retain and analyze these signals to produce intelligence information. This system is explained, in technical detail, in an NSA document entitled the Radio Signal Notation (Rasin) Manual.

25X1, 3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

25X1, 3 and 6, E.O.13526

Withheld from public release under
§6 of the National Security Act of 1959,
50 U.S.C. 3605 (P.L. 86-36)

25X1, 3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

d. The defendant has admitted that he was specifically tasked by his coconspirators to acquire a complete, unedited version of the "Rasin Manual," and the corresponding Catalogue, and in fact did so.

25X1, 3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

25X1, 3 and 6, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

25X1 and 6, E.O.13526

8. [redacted] TECHNOLOGY OF SOVIET WEAPONS AND RADAR SYSTEMS.

Since much of the military technology used by powers unfriendly to Israel is of Soviet origin, there is a natural desire by Israel to obtain as much information as possible concerning that technology.

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

9. [redacted] POLITICAL-ECONOMIC AFFAIRS OF MIDDLE EASTERN NATIONS.

The ability of a nation to successfully prosecute a war or to successfully carry out its foreign policy objectives depends in large part on its industrial base, on the will of its people and on its political leadership. Accordingly, political and economic studies of nations are vitally important for contingency planning purposes. Some brief examples of the types of political and economic information which were sold by defendant, [redacted]

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

10. Intelligence information

25X1 and 6, E.O.13526

Because most finished intelligence product is "cleansed" of identifying sources of the information obtained, it is sometimes difficult or impossible to determine the original source of data underlying a report.

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X3, E.O.13526

Withheld from public release under
§6 of the National Security Act of 1959,
50 U.S.C. 3605 (P.L. 86-36)

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

12. [redacted] Middle Eastern ORDERS OF BATTLE.

It needs little explanation to comprehend the importance, from the Israeli perspective, of having available all information possible concerning the fighting capabilities of other Middle Eastern nations. To know the capabilities of the adversary is to understand the requirements for defeating or avoiding those capabilities in the accomplishment of one's own objectives. I have chosen only a few of the documents gained by Israel from the defendant:

[redacted]

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

PART TWO
DAMAGE TO THE NATIONAL SECURITY

25X1 and 6, E.O.13526

14. [redacted] As noted previously, the breadth of the disclosures made by the defendant was incredibly large. Accordingly, the damage to U.S. national security interests resulting from those activities is similarly broad. I will detail herein, the more pertinent aspects of damage to U.S. national security as I perceive them:

a. Damage to Intelligence Sharing Agreements.

Since the activities of the defendant impact directly on U.S. intelligence activities, it is appropriate to begin with intelligence. It should be obvious that the United States has neither the opportunity nor the resources to unilaterally collect all the intelligence information we require. We compensate with a variety of intelligence sharing agreements with other nations of the world. In some of these arrangements there is virtually a full partnership which stems from recognition of common and indelible interests. Most, however, are fashioned on a quid pro quo basis. For example, the United States agrees to share with an ally certain types of intelligence information in exchange for desired information or other valuable assistance. Further, once such agreements are entered into, decisions to disclose particular classified documents or items of intelligence information are made by high level officials after a careful evaluation of the costs of

disclosure to our national security versus the benefits expected to be obtained if disclosure is approved. In some instances, especially sensitive intelligence information that is sought by an ally is traded because the ally agrees to furnish equally sensitive information vital to U.S. security interests. The general harm I perceive to have come to U.S. intelligence sharing capabilities from the defendant's activities stems from three different categories of intelligence partnerships.

1) Between the United States and Israel

25X1 and 6, E.O.13526

2) Between the U.S and Middle Eastern Nations.

Although the United States has no formal allies among Middle Eastern nations, we do have firm friends.

25X1 and 6, E.O.13526

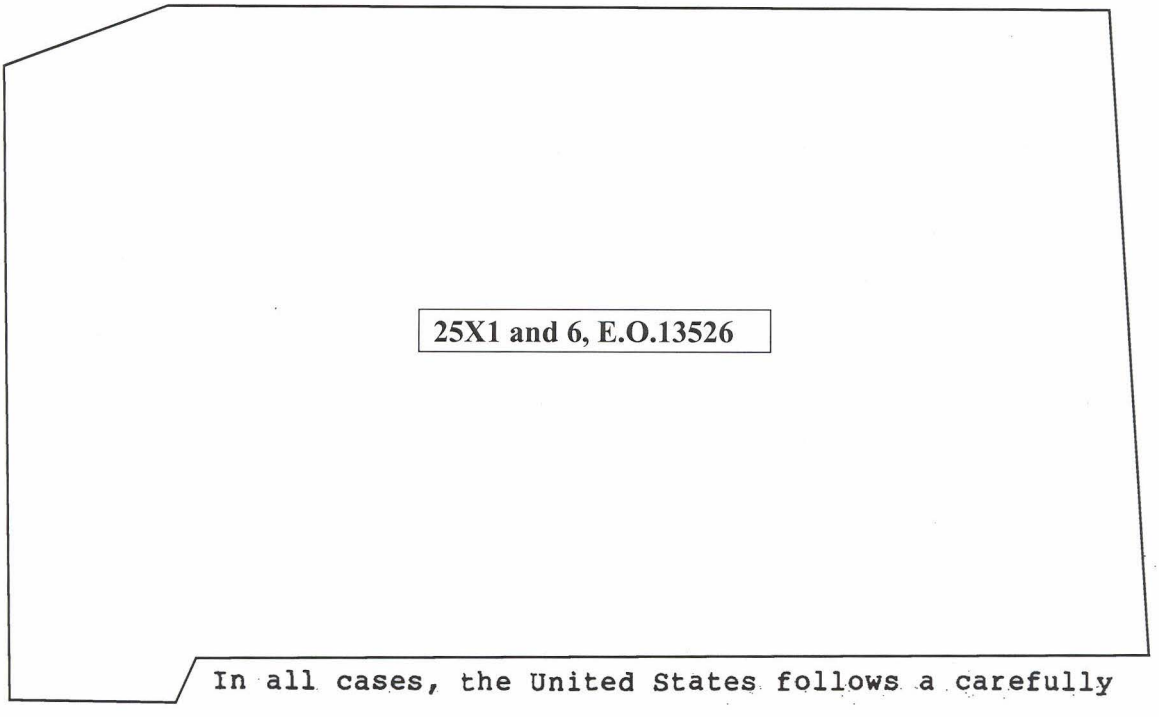
25X1 and 6, E.O.13526

3) Between the U.S. and other Allied Nations.

Since the United States does have a broad base of intelligence sharing arrangements, it is inevitable that some information gleaned from allies was included in that passed to Israel. This has created a perception that the U.S. is unable to protect the information given us and may well serve as a catalyst to curtail information received from allies in the future. Of course, it is impossible to be certain whether this will be a problem, because we will never know what we have not been given. Clearly, however, there is a significant possibility of degradation to our intelligence gathering apparatus, particularly since many of our arrangements are predicated on the fact that we have agreed to hold such arrangements secret.

25X1 and 6, E.O.13526

b. Damage to U.S. disclosure policy with respect to Israel



In all cases, the United States follows a carefully conceived policy, with stringent parameters of permissible disclosure. An explanation of those parameters follows:

1) POLICY. Classified military and intelligence information are national assets which must be conserved and protected and which will be shared with foreign entities only when, by doing so, U.S. policies are advanced. In every case, a final decision to release a specific item of classified information to any foreign power may be made only by a responsible U.S. authority, and only when (1) sources and methods of acquisition are not subjected to an unacceptable risk of disclosure; (2) the U.S. will receive an identifiable benefit from release of the information to the foreign power;

(3) disclosure is consistent with U.S. national defense and foreign policy objectives; (4) there is a demonstrated need for the recipient to receive the information; (5) disclosure is consistent with previous disclosures to the same foreign power; and (6) the recipient can afford the information substantially the same degree of security protection given it by the United States.

2) EXAMPLE. The United States frequently discloses classified information to foreign powers, but always in conformance with the basic criteria set forth above. It is ironic that the stringency of applying these criteria may, perhaps, be best illustrated by reference to the specific case of Israel. The unique relationship between the United States and Israel is understood world-wide.

25X1 and 6, E.O.13526

Applying the criteria for disclosure, however, the Department of Defense strictly limits disclosures of classified military information.

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

However, before such information is disclosed, each of the six criteria must be considered.

25X1 and 6, E.O.13526

3) Proper applicaton of all six criteria for foreign

disclosure is vitally important for U.S. interests because all criteria must be balanced against one another. For example, the requirement to protect sources and methods of information acquisition, as well as the requirement to protect the substantive information received, must conform with the recipients "need" for that information and the expectation of benefit for the United States. This usually means that substantive information is redacted from the original documents containing the information prior to disclosure. The result is

25X1 and 6, E.O.13526

In this case, the defendant unilaterally defeated U.S. disclosure policies. He not only provided classified information to Israel, which Israel was not authorized to receive, but in doing so, he furnished original source documents which had not been "sanitized," thus substantially compounding the harm.

The defendant has specifically identified more than 800 U.S. classified publications and more than 1,000 U.S. classified messages and cables which he sold to Israel. Of

25X1 and 6, E.O.13526

To the best of my knowledge, not one of the publications he provided them was authorized for official release to Israel in unredacted form.

15. [redacted] The actions of the defendant have jeopardized the substantive intelligence information he provided to the Israelis, as well as the sources of that information, by placing it outside of a U.S. controlled security environment.

25X1 and 6, E.O.13526

The United States, and virtually all of those who cooperate with us by sharing intelligence, have developed a system of protecting classified information which depends on the reliability of individuals for its effectiveness. It is also a system which varies its requirements for protection with the sensitivity of the information at stake. All classified material is required to be placed in proper storage, appropriate to its classification level, and all personnel who have custody are accountable for ensuring that proper procedures for protecting it are followed. The system necessarily depends on the integrity and reliability of the individual. So long as an individual is accountable for classified material in his custody, we can generally assume that personal interest will guarantee its safekeeping. It is when an individual obtains custody of classified material for

which he is not responsible that safekeeping is jeopardized. In such an instance, there is no real incentive to adequately protect such information. One example of an occasion when this happens in the normal course of business is the necessary use of couriers to carry highly sensitive information from one location to another. The defendant frequently acted as such a courier, and it was his abuse of this system, a system necessarily dependent on the integrity of the individual, which permitted his espionage activities to occur. Moreover, in a situation such as this one, there is every incentive to use the acquired information in a person's self interest. Examples of my reasoning follow:

a. The defendant provided to the Israelis various information relating to the Libyan Air Force. Further, the defendant told us he was informed by his Israeli handlers that information he provided was instrumental both in enabling a successful strike on PLO headquarters in Tunisia and in avoiding contact with Libyan Air Forces. From my perspective, this situation provides poignant insight to the problem of unlawful disclosure of national security information.

1) First, it illustrates a point I made earlier. If one nation understands the order of battle of another, adversary nation, it has information necessary to defeat or avoid its adversary. Thus, the likelihood of armed conflict becomes greater. In this case, the Israel Air Force was able

to strike its target in Tunisia with an unusually high probability that they would not be intercepted by hostile aircraft. However, the resultant damage and loss of life worked, in my opinion, to the detriment of the United States. In all, approximately 62 Palestinians and 27 Tunisians were killed in the raid, and some 150 others were wounded.

2) Second, the Israeli strike was directed against a power friendly to the United States. The Middle East has been a volatile region for many decades, but Tunisia has often acted as an "honest broker" for the United States.

25X1 and 6, E.O.13526

3) Several years ago when Israel was in occupation of a significant part of Lebanon, and was insisting that the PLO be removed from Lebanon prior to Israeli withdrawal, the emotional climate in the Middle East became explosive because no "home" could be found for the PLO. Tunisia, prompted by the United States, volunteered to accept the PLO in order to "defuse" the political/military situation in Lebanon. I think it clear that significant potential hostilities and bloodshed were thus avoided by Tunisia's humanitarian gesture. In light

of the defendant's unlawful disclosures, the good offices of Tunisia can no longer be counted on as they have been in the past. In any event, it is crystal clear that the raid on the PLO in Tunisia was contrary to the national interest of the United States.

b. Significant amounts of the information passed by the defendant related to weapons systems and military capabilities. For example, he provided information on Soviet built air-to-air missile systems and on Middle East air orders of battle. Since Israel depends for its national security on control of Middle East air space, much of this information was considered vital, and, as Col. Sella remarked, was not previously possessed by Israel.

25X1 and 6, E.O.13526

~~TOP SECRET~~ UMBRA

25X1 and 6, E.O.13526

c. One danger inherent in all security concerns is that of penetration by a foreign agent. We in the United States have been made all too aware of this risk in the past year; the defendant is a case in point. We cannot be secure even with the knowledge that the information passed by the defendant was provided to an ally who has security procedures as stringent as our own. All such systems are vulnerable.

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

16. [redacted] Of similar concern is the potential damage to U.S. interests which may be caused should Israel pass the intelligence acquired through the defendant to third parties.

[redacted]

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

7. [redacted] In my judgment, the actions of the defendant have caused a high probability of harm to the foreign relations of the U.S. with friendly Arab nations. I believe the rationale for this judgment is sufficiently clear from my preceding statements that I will simply list some of the specific,

potential causes of a worsening of U.S.-Arab relations.

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

18. [redacted] I cannot overemphasize that the United States strives hard to promote peace and stability in the Middle East. In doing so, it is not unusual that Israel and the U.S.

find themselves with differing approaches and perspectives.

25X1 and 6, E.O.13526

I believe that the defendant's disclosures have had, and will continue to have, an adverse impact

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

25X1, 3 and 6, E.O.13526

Withheld from public release under
§6 of the National Security Act of 1959,
50 U.S.C. 3605 (P.L. 86-36)

PART THREE
THE SIGNIFICANCE OF THESE DISCLOSURES

25X1 and 6, E.O.13526

21. [redacted] HARM TO U.S. FOREIGN POLICY:

In my opinion, the defendant's unlawful disclosures to the government of Israel have harmed U.S. foreign policy. My conclusions flow directly from the information I have discussed previously.

25X1 and 6, E.O.13526

25X1 and 6, E.O.13526

22. [ ] COMPROMISED SOURCES AND METHODS:

I will not repeat the difficulties in reacquiring damaged sources of intelligence acquisition which have been compromised.

25X1 and 6, E.O.13526

23. [redacted] RISK TO U.S. PERSONNEL:

Finally, the United States must expect some amount of risk to accrue directly to U.S. persons from the defendant's activities. [redacted] concomitant risk with which I, as Secretary of Defense, am particularly concerned, is that U.S. combat forces, wherever they are deployed in the world, could be unacceptably endangered through successful exploitation of this data. [redacted]

25X1 and 6, E.O.13526

24. (U) I have provided the foregoing statements to provide

my views of the significant harm caused to national security by the defendant and as an aid to the Court. The data provided represents my opinions and conclusions stemming from my review of the data compromised, as well as from information obtained by me in my capacity as Secretary of Defense and as a member of the National Security Council. The defendant has substantially harmed the United States, and in my view, his crimes demand severe punishment. Because it may not be clear to the court that the defendant's activities have caused damage of the magnitude realized, I felt it necessary to provide an informed analysis to the Court so that an appropriate sentence could be fashioned. My foregoing comments will, I hope, dispel any presumption that disclosures to an ally are insignificant; to the contrary, substantial and irrevocable damage has been done to this nation. Punishment, of course, must be appropriate to the crime, and in my opinion, no crime is more deserving of severe punishment than conducting espionage activities against one's own country. This is especially true when the individual spy has voluntarily assumed the responsiblity of protecting the nation's secrets. The defendant, of course, had full knowledge and understanding of the sensitivities of the information unlawfully disclosed. To demonstrate that knowledge, I have attached copies of non-disclosure agreements which he voluntarily executed. Should the Court require further

information or explanation of anything contained herein, you may provide the bearer of this document with your requirements and I will respond to them.

Under penalties of perjury, I hereby declare the foregoing statements to be true and correct to the best of my knowledge information and belief.

Executed this 8th day of January 1987.

Caspar W. Weinberger

Caspar W. Weinberger

Copy 1 of 9 Copies.
Page 46 of 46 Pages.

GLOSSARY

1. TOP SECRET (TS): Information which if inappropriately disclosed would cause exceptionally grave damage to the national security of the United States.

2. SECRET (S): Information which if inappropriately disclosed would cause serious damage to the national security of the United States.

3. CONFIDENTIAL (C): Information which if inappropriately disclosed would cause damage to the national security of the United States.

4. WARNING NOTICE -- INTELLIGENCE SOURCES OR METHODS INVOLVED (WNINTEL): This marking is used on intelligence information which identifies or would reasonably permit identification of an intelligence source or method which is susceptible to countermeasures that cold nullify or reduce its effectiveness. Information so designated may not be disseminated in any manner outside authorized channels wiothout the permission of the originating agency and an assessment by the senior intelligence officer of the disseminating agency as to the potential risks to the national security and to the intelligence sources and methods involved.

5. DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON): This is the most restrictive marking of intelligence information and is used to enable continuing knowledge and supervision by the originator of the use made of the intelligence information so marked. Information bearing this marking may not be disseminated in whole or in part through briefings, incorporation into reports, or in any other manner outside the headquarters elements of the recipient organization, or used in investigative actions, without the advance permission of, and under conditions specified by, the originator.

6. NOT RELEASABLE TO CONTRACTORS/CONSULTANTS (NO CONTRACT): This marking is used to identify classified intelligence that shall not be released to contractors or consultants without the permission of the originating agency. It is designed to prevent a contractor from unfairly gaining a competitive advantage or to avoid creating a conflict of interest.

7. NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN): This marking is used to identify classified intelligence information that may not be released in any form to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator. It may be used on intelligence which if released to a foreign government or national(s) could jeopardize intelligence sources or methods, or when it would not be in the best interest of the United States to release the information from a policy standpoint upon specific determination by the cognizant senior intelligence officer of the disseminating agency.

8. TOP SECRET CODEWORD (TSC): Top Secret information derived from intelligence sources and methods. The TSC information referred to in this affidavit derives from signals intelligence sources and methods and is currently designated by the distinctive codeword UMBRA (C-CCO).

9. SECRET CODEWORD (SC): Secret information derived from intelligence sources and methods. The SC information referred to in this affidvit derives from signals intelligence sources and methods and is currently designated by the distinctive codeword SPOKE (C-CCO)

10. COMINT CHANNELS ONLY or HANDLE VIA COMINT CHANNELS ONLY (CCO/HVCCO): This marking is used to identify classified communications intelligence (COMINT) information which does not reveal the success or failure of a cryptologic process (FOUO).