STEWART SECURITY SERVICES
Crystal House I, Apt. 202
1900 South Eads
Arlington, Virginia 22202

(703) 979-6540
Security Consultant - Investigations

W. Donald Stewart, President

February 24, 1978

Statement by Mr. W. Donald Stewart

on

The Security Clearance Program
and Its Relation to Possible
Unauthorized Disclosures of Classified Defense Information

for

The Senate Select Committee on Intelligence

I N D E X

Approved For Release 2001/11/08 : CIA-RDP81-00142R000700040003-1

The Security Clearance Program and Its Relation to Possible Unauthorized Disclosures of Classified Defense Information

Unauthorized Disclosures of Classified Defense Information

This statement is being voluntarily furnished by W. Donald Stewart to the Senate Select Committee on Intelligence specifically for the attention of the Subcommittee on Secrecy and Disclosure.

Qualifications of Author

I served as an FBI Agent from July 1951 until August 1965, the last nine years as an Espionage Supervisor at FBI Headquarters, and from August 13, 1965 until December 1972 as Chief Investigator for the Office of the Secretary of Defense with the primary responsibility of investigating Unauthorized Disclosure cases. Because the Directorate for Inspection Services (DINS), commonly known then as the Secretary of Defense's Inspector General group, was phased out for economy purposes, I was appointed Inspector General of the newly formed (October 1972) Defense Investigative Service where I remained until I retired on June 30, 1975. During my tenure in DINS I handled 222 Unauthorized Disclosure investigations and numerous major criminal and counterintelligence investigations in accordance with the provisions of Department of Defense Directive 5210.50 entitled "Investigation of and Disciplinary Action Connected with Unauthorized Disclosures of Classified Defense Information" dated April 29, 1966, which made DINS the focal point of all such violations, and with the provisions of Department of Defense Instruction 5200.22 entitled "Reporting of Security and Criminal Violations" (to DINS) dated September 12, 1966.

In April 1969 I prepared a pamphlet entitled "Analysis of Unauthorized Disclosure Investigations." This consisted of a review of 125 investigations conducted between March 1965 and March 1969. I described the whole program - Background, Authority, Source of Unauthorized Disclosures, Mechanics of Handling, Program Improvement, Positive Results, Personality Characteristics of Individuals Responsible for Unauthorized Disclosures, the Question of Prosecution, and Observations.

Since I retired I have written a book entitled "Leaks" (not yet published) and founded Stewart Security Services.

Purpose

The purpose of this paper is twofold. One purpose is to show how haphazard the Security Clearance Program operates, and secondly to show that weaknesses in our Security Clearance Program could be responsible for unauthorized disclosures of classified information through the improper conferring on of a security clearance on an undeserving person

or through the failure to remove a person's security clearance when the person becomes a security risk for one of several reasons.

Specifically, this paper reflects who has access, legally and illegally, to classified Defense data; examples of weaknesses in our Security Clearance Program permitting undesirables to obtain a security clearance; variations in the investigative criteria for a Top Secret clearance; how security clearances are adjudicated, along with an idea for a Central Adjudication Branch for economy, security and privacy purposes, and finally the introduction of the use of the polygraph for pre-employment checks and for background checks. The polygraph could minimize invasion of an individual's privacy, expedite his date of employment and clearance, and save the U.S. Government a large amount of money in various ways.

Hopefully, the Committee will recognize the need to bring the entire Security Clearance Program into proper focus with appropriate standardization and safeguards to all persons concerned.

The Meaning of a Security Clearance

What does a security clearance mean? Actually it means that a designated authority has sanctioned a person's access to view classified defense material at a level of Confidential, Secret, or Top Secret. Actually there are also what are called "Exotic" clearances or "Special" clearances which are over and above Top Secret.

Who Has Access to Classified Data

(A) The Press

The press does not, in fact, legally get a security clearance; however, they are often given "Backgrounders," which are familiarization lectures in order to prepare them to write a story. These generally contain classified defense information. There is a stipulation that the data imparted is "Off the Record." In 1969, there was a case where a Vice Admiral compromised our 10-year lead over the Soviets on Anti-Submarine Warfare. Reportedly the press was not told the "backgrounder" was "off the record" and 14 papers ran the story. But, then again, what authority exists by anyone to confer a clearance on any member of the press through a "backgrounder," "off the record." When members of the press are taken into the Defense Department's Office of Public Affairs, a Top Secret background investigation is conducted before the clearance is conferred.

What proof of identification must he have to enter the service and later obtain his Secret clearance? He must produce a high school diploma and a birth certificate. Are they verified? Yes, the military recruiter causes checks to be made at the high school and the appropriate Bureau of Vital Statistics. What does that do? It merely informs the recruiter that John Jones graduated from Holy Mount High School - it does not tell the recruiter if John Jones is white or black, tall or short, blonde or redheaded. The Bureau of Vital Statistics merely informs that one male was born on such and such a date to William and Doris Jones, perhaps it might gratuitously give the baby's name as John. Can the required documentation be fabricated? Yes, I've had a couple of national news stories on this weakness in our security program, but to no avail. Additionally, no change has been made even in view of the fact that last summer it was discovered that 500 Panamanian aliens enlisted in the U.S. Marine Corps by utilizing fabricated documents. Can this be stopped? Yes, by requiring the enlisted to submit the names and addresses of three references who should be interviewed to verify the John Jones is the person he purports to be, and also to have the FBI do a search of his fingerprints from the fingerprint card he submits.

Do you have any examples of people entering the service illegally other than the above 500 Panamanians? Yes, about two years ago I had a national news story about Thomas Ragner Faernstrom who reenlisted fictitiously ten times during a 13-month period between November 1973 and January 1975, collecting approximately $30,000 in bonus. Subsequent interviews with him revealed he had done this over a 10-year period and bilked the U.S. Government out of $600,000. A check of his fingerprints would have uncovered him at any stage.

Last July a 28 year old North Carolina man was arrested and held 40 days as a deserter from the Army in spite of his protests that he never joined. Someone else joined using his identification which he had previously lost. An FBI fingerprint check would have probably nipped this fraudulent enlistment in the bud at the enlistment stage as the fraudulent enlistee most likely couldn't get in under his own identity.

In January 1975, a sailor in Seattle, Washington hi-jacked a Navy plane and was subsequently caught. Later it was developed that a year before he had been discharged from the Marine Corps as a mental case. An FBI fingerprint check would have surfaced him.

Actually on the subject of poor security I have acted in the capacity of a one-man vigilante committee before I retired and for 2-1/2 years since without success. I could cite example after example, but the purpose here is not to show how the vulnerability to our security exists from the fact that you are an accepted person. Since you live with people who have Top Secret clearances, they are likely

to impart data to you because you are a serviceman like them. Further, you have a legitimate right to be in the proximity of certain areas which contain Top Secret data and are likely to learn about them because you are accepted as another service person. Actually, one service person does not enter a room and say, prior to a conference, "Who's got Top Secret here? I want to 'shoot my mouth off'."

The 500 illegal Panamanian aliens who joined the U.S. Marine Corps undoubtedly got some exposure that probably the Marines wish they hadn't. Further, wouldn't it be ironic if our U.S. Marine Corps became engaged later in a battle in Panama and met stiff resistance and learned later the enemy was trained in our U.S. Marine Corps camps? Hopefully that won't happen.

(D) Civilian Employees

Civilian employees and Department of Defense contractor employees have access to classified information. Most are awarded a Secret clearance on a straight National Agency Check (NAC). If, however, any derogatory data develops, an investigation is undertaken to resolve the matter.

Civilian employees requiring a Top Secret investigation undergo a thorough background check involving verification of birth data, residencies, employment, and interviews of references.

Variations in the Investigative Criteria for a Top Secret Clearance

The FBI, Defense Investigative Service (DIS), and the Civil Service Commission (CSC) each do background investigations for Top Secret clearances. Possibly State Department and the CIA also do their own. However, my point is that the criteria differ and to this end I'll speak of the variations in the FBI, DIS, and CSC criteria for a Top Secret clearance.

If there is any specific interest here, I have written a detailed paper dated February 25, 1975 entitled "Criteria for Security Clearances" where I go into greater depth. Briefly, the FBI is the only one of the three which is recognized as a police agency and thereby permitted to review all police agency criminal files in checking for a reference to the person being cleared for Top Secret. This being so, why do we worry about a person being a homosexual in connection with his getting a clearance since DIS and CSC are not likely to surface this data? As you may know, most homosexual subjects are often booked by a police department in the category of "Disorderly Conduct," given a small fine and released. For example, a former Special Assistant to former President Lyndon Johnson was arrested at a YMCA in Washington, DC, in about 1963, for his

participation in a homosexual affair. If this affair had happened in New York City, for example, and DIS or CSC had been conducting a background check based on the fact that Jenkins lived in New York once, neither having access to NYPD files could have uncovered this arrest, but, of course, the FBI, having such access, would have the data, would probably have caused him to be denied a clearance as a possible security risk. There are also other crimes which would not necessarily cause the person's fingerprints to be forwarded to FBI Headquarters and his arrest would go undetected during a fingerprint check of FBI files.

Let's look at the scope of an investigation. The FBI does neighborhoods for only the last five years unless derogatory data is developed. DIS and CSC go back for 10-15 years. The FBI verifies birth data from records and not Bureau of Vital Statistics' records as does DIS and CSC. FBI checks three listed references and no developed references are sought unless derogatory data is developed. If a listed reference is not available when the FBI knocks on his door, no effort is made to locate him again. DIS and CSC locate all listed references if possible.

The House Appropriations Committee hearings in April 1975 reflected that based on its review of DIS and CSC from May 1974 to November 1974, the following was noted. DIS charged $390/investigation and CSC charged $604. At that time FBI charged $799. DIS cases averaged 19.8 leads/case whereas CSC averaged 30.7. DIS reports averaged four pages and CSC averaged 21 pages. FBI then operated under a 30-day deadline whereas DIS and CSC were taking in the neighborhood of 45-60 days. In regard to updating Top Secret clearances, FBI never updates those of its personnel; CIA updates its personnel every 3-5 years, and the Defense Department does a 5-year bring-up.

Adjudications

Who decides who gets the clearance after the background investigation is done? The Defense Investigative Service at one time serviced 1400 customers. That meant that each customer would get a full background investigation on its person and determine if he or she qualified for a clearance. I can't personally state that much additional investigation was often requested because the adjudicator wouldn't make a decision on the facts available. Yet, more than likely another adjudicator in the same agency could have - that's the difference between experience and lack of it.

Most important is the fact that the 1400 agencies had in their files much personal data on the person being cleared and this data, in my opinion, should not be in the files of the agency. The natural solution would be a Central Adjudication Branch within DoD,

employee, a new recruit must be found. Secondly, in a case that homosexuality may be developed during an investigation, a polygraph with the applicant would reflect deception and confronted with same the person might make a full disclosure. The alternative to his lack of cooperation on that subject or other subjects of possible personal embarrassment is to resolve the derogatory data in a full field investigation. Even if the person is determined not to have committed the suspected act, be what it may, the line of questioning pursued in neighborhoods where the person now lives and formerly lived, as well as present and past employment, leaves him with a stigma.

In the case of the military enlistee, the polygraph again being used to just verify what the enlistee has told us becomes an excellent screening device and may even serve to expedite his entrance into the service. On the other hand, at the recruiter level, the utilization of a polygraph at the recruiter level may also surface a potential fraudulent enlistee, thereby saving the U.S. Government a great deal of money by eliminating associated cost with processing and training a recruit. The polygraph could indicate that the potential recruit is or has been a drug user, is presently a fugitive from justice, or has served time for a crime which would disqualify him from military service, is not the person he purports to be, has certain physical limitations, etc. Again, only his questionnaire is being reviewed with him.

In a July 8, 1976 Los Angeles Times newspaper article entitled "At Least 1 in Every 250 Recruits Enlisted Fraudulently, Pentagon Figures Disclose" by Norman Kempster, 1,935 cases of fraudulent enlistments came to the attention of the military during a 15-month period ending March 31, 1976. What the article does not bring out is that these people for the most part surfaced themselves in order to get discharged. We have to admit that when economic conditions are not the best that the $403/month pay, plus room and board and a clothing allowance for a Private in the military, can look awfully good.

Locally I can think of Army Private Angel, who killed two Montgomery County (Maryland) police officers after a bank robbery about two years ago as being one of the persons falling into the fraudulent enlistment group. He was not truthful in the papers he executed before entering the service. Whether it would or would not have altered the death of the two Montgomery County police officers, I cannot say. I can say that a pre-enlistment screening by polygraph would probably have excluded him and saved the Army a great deal of time and expense associated with his induction and training and embarrassment to its service. Angel was also a suspect in a murder prior to entering the service.

for example, which would handle and retain all background investigative reports and simply inform the customer that based on the results of the background investigation the Department of Defense is awarding John Jones a Secret or Top Secret clearance. Much is saved in logistic costs in this manner because every agency doing its own adjudication must have its own classified file room complete with personnel. Also, many potential invasion of privacy suits could be avoided because personal background data would be much more restricted. No one at the agency has any need to know personal type data offered during the investigation about one of the employees being cleared. I personally have had complaints from employees about the discussion of such personal data such as age, past marriages, etc., contained in investigative reports on Personal History Questionnaires executed by the person being cleared.

The Polygraph for Security Screening

When the idea of using a polygraph is mentioned, instant resentment takes place. Immediately every one thinks in terms of its use being to convict someone; however, the polygraph is often used for exculpating purposes. Also, it is used for a veracity check such as was recently done during the interviews in Korea with Tongsun Park. Its use in connection with the Justice Department interviews of Park more or less set a precedent as far as the Government is concerned in that it places a great deal of belief in the ability of the polygraph to show deception which does not necessarily mean guilt.

Now, let's consider using the polygraph for general security screening. What I would propose is simply taking in hand the Personnel Security Questionnaire, FD 398, which all persons requiring a clearance must execute, and one by one reviewing each question with the applicant. For instance, is your name John Jones? Were you born April 10, 1928 at New York, New York? Have you ever been arrested? Did you reside at 1212 Vermont Avenue, Ventnor City, New Jersey from 1964-1972? etc. This is not an invasion of privacy since we are only reciting what the applicant has told us. We are not going to disqualify him if he shows deception on the above residence question and arrest question. We are going to instruct the field investigator to dig into these areas. We may very well be able to eliminate all other areas if no deception is noted.

What is the advantage of the polygraph in this type of screening? There are several. One is probably a quicker clearance for a pre-employment check enabling the person to report to work earlier. Often while the U.S. Government is checking out someone, the person becomes tired of waiting and gets other employment; hence, all the investigative effort is lost and if the person was to become a Government

Another point, not only in favor of expediting the investigation of a civilian or military employee and saving related costs, is that many areas where a person may have formerly resided or was employed are now considered "high risk" areas and are not normally entered by Defense Investigative Service agents because of possible personal jeopardy. Therefore, to develop the fact a person lived there or worked there, other investigation must be launched to verify same. A similar but less dangerous type of a case is one where a person has listed a residence or employment, necessary to be verified being in that part of this country which is 400-500 miles from the nearest investigative office, making it necessary for an investigator to take a road trip to the location. A polygraph might well resolve our interests in this matter.

In closing, I believe our present Security Clearance Program and pre-employment check could be upgraded by use of the polygraph. At the same time in many cases there would be a substantial saving to the U.S. Government and a minimum of invasion of privacy to an applicant.

DD/A Registry
File ~~Signed~~
Security 5-1

	UNCLASSIFIED		CONFIDENTIAL		SECRET

EXECUTIVE SECRETARIAT

Routing Slip

TO:		ACTION	INFO	DATE	INITIAL
1	DCI		X w/ref		
2	DDCI		X w/ref		
3	DDA	X			
4	LC		X		
5					
6					
7					
8					
9					
10					
11					
12					

SUSPENSE _____
Date

Remarks: To 3: In his memo of 22 February, the DCI sent along to you Mr. Stewart's earlier testimony before the SSCI. The attached is provided for your information and appropriate action in that context.

[redacted]
Executive Secretary
28 Feb 78
Date

3637 (10-77)

STATINTL

D/OS - 3/3/78

ROUTING AND TRANSMITTAL SLIP 78-4468/1

TO	INITIALS	CLASSIFICATION
Adm Stansfield Turner	DATE	COORDINATION
2 Director	INITIALS	FILE
	DATE	INFORMATION
3 C/A. Washington, D.C 20505	INITIALS	NOTE AND RETURN
	DATE	PER CONVERSATION
4	INITIALS	SEE ME
	DATE	SIGNATURE

REMARKS

Dear Adm. Turner

Thank you for your letter of Feb 21 concerning receipt of my statement of Feb 3 1978 to the Senate Select Committee on Intelligence.

Attached is another paper I have just prepared for the Committee, Hoping it is of interest

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

STATINTL FROM [redacted] DATE PHONE

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41CFR) 100-11.206

★ GPO : 1969 OF—332-829 5041-101

STEWART SECURITY SERVICES
Crystal House I, Apt. 202
1900 South Eads
Arlington, Virginia 22202

W. Donald Stewart, President

(703) 979-6540
Security Consultant - Investigations

Feb 3, 1978

Admiral Stansfield Turner
Director C/IA.
Washington D.C. 20505
~~Langley, Virginia~~

Dear Admiral Turner,

On January 24, 1978, I was interviewed by Mr. Mark Gitenstein, a Staff Counsel on the Sub-Committee for Secrecy and Disclosure, a part of the Senate Select Committee on Intelligence. I was later asked by him to prepare a statement.

Attached for the interest of C/IA is a copy of my statement, at least I feel I am trying to "turn off" leaks.

Sincerely

W. Donald Stewart

STEWART SECURITY SERVICES
1300 South Eads
Arlington, Virginia 22202

W. Donald Stewart, President

(703) 979-6540
Security Consultant - Investigations

FEBRUARY 3, 1978

STATEMENT BY MR. W. DONALD STEWART

ON

UNAUTHORIZED DISCLOSURES OF CLASSIFIED DEFENSE INFORMATION

FOR

THE SENATE SELECT COMMITTEE ON INTELLIGENCE

INDEX

Unauthorized Disclosures of Classified Defense Information

This statement is being voluntarily furnished by W. Donald Stewart for the benefit and interest of the Senate Select Committee on Intelligence.

Qualifications of Author

I served as an FBI Agent from July 1951 until August 1965, the last nine years as an Espionage Supervisor at FBI Headquarters, and from August 13, 1965 until December 1972 as Chief Investigator for the Office of the Secretary of Defense with the primary responsibility of investigating Unauthorized Disclosure cases. Because the Directorate for Inspection Services (DINS), commonly known then as the Secretary of Defense's Inspector General group, was phased out for economy purposes, I was appointed Inspector General of the newly formed (October 1972) Defense Investigative Service where I remained until I retired on June 30, 1975. During my tenure in DINS I handled 222 Unauthorized Disclosure investigations and numerous major criminal and counterintelligence investigations in accordance with the provisions of Department of Defense Directive 5210.50 entitled "Investigation of and Disciplinary Action Connected with Unauthorized Disclosures of Classified Defense Information" dated April 29, 1966, which made DINS the focal point of all such violations, and with the provisions of Department of Defense Instruction 5200.22 entitled "Reporting of Security and Criminal Violations" (to DINS) dated September 12, 1966.

In April 1969 I prepared a pamphlet entitled "Analysis of Unauthorized Disclosure Investigations." This consisted of a review of 125 investigations conducted between March 1965 and March 1969. I described the whole program - Background, Authority, Source of Urauthorized Disclosures, Mechanics of Handling, Program Improvement, Positive Results, Personality Characteristics of Individuals Responsible for Unauthorized Disclosures, the Question of Prosecution, and Observations.

Since I retired I have written a book entitled "Leaks" (not yet published) and founded Stewart Security Services.

Three Types of Unauthorized Disclosures

From December 1972 until present I have continued to follow unauthorized disclosure matters in the press and have amassed a file of public source information. My experience has led me to conclude that there are three types of unauthorized disclosures of concern; namely, the Overt, Covert, and Potential. These will be described in the section entitled "Discussion." But briefly the Overt types are those we read about in the newspapers and fall into one of eight categories of leaks also set out in the "Discussion" section. The Covert types are ones we know little about until an informant advises someone is attempting to provide enemy foreign intelligence with classified Defense data. The third type, Potential, is one which I speculate that few have little knowledge of because there is no mechanism for reporting these and, until the advent of the above DoD Instruction 5200.22, even the Secretary of Defense would remain uninformed. This type develops from civilian or military personnel who have become disenchanted. Each person has the potential of orally disclosing Classified data to enemy foreign intelligence. Additionally, another Potential type of disclosure can result from a lost Classified document, such as in one case of the lost Atomic Stock Pile Reports.

Security Problem

Our main security problem concerning "leaks" is that there is no one in overall charge of leak matters in the U.S. Intelligence program which presently operates like amateur night. Each U.S. agency and military department operates independently of each other with practically no internal coordination. Matters of national security interest are often buried rather than have the military department or Government agency suffer any embarrassment resulting from a "goof" by one of its employees.

Within the Defense Department, there is no such group as an Intelligence Security Advisory Board to specifically determine direct appropriate action concerning DoD personnel who pose a threat in that they might compromise highly classified intelligence data. Not having committed a crime, prosecution is not the solution and, after the potential crime has been committed, the person may not be around to prosecute. We have had some potentially serious such cases which are mentioned in Potential Leaks in the Discussion section. Neither the FBI nor the CIA is normally notified. Some persons have been discharged to solve the military commander's problem. One was "granted immunity" to confess an espionage contact by the person's Commanding Officer, such immunity is normally the prerogative of the Justice Department.

A second offering is that the Select Senate Intelligence Committee make itself or some other appropriate body the focal point for reporting all occurrences of and investigations of unauthorized disclosures of classified data. This body would then be in a position through monitoring to force a determination of whether the classified data in question couldn't be declassified now or later for prosecution purposes. This would insure in most cases that the violations received a review by the Justice Department. In all due respect, most General Counsels of concerned agencies often know little about this type of Federal law, including the possibility of prosecutions under the Conspiracy to Commit Espionage Act, but often usurp the Justice Department's prerogative by rendering their own opinion that the case can't be prosecuted.

If there was an office, such as DINS, with the responsibility to oversee all leak investigations, it would be able to insure an investigation was not prematurely aborted when the next obvious lead might very well surface the culprit, as has often happened.

DINS (Directorate for Inspection Services) did function in focal point manner within DoD and it was able to force more investigative effort from the military services than it intended and such pressure often was beneficial.

Lastly, the enactment of some type of In Camera judicial procedure would be most helpful and could be reserved for special cases. It could be an outstanding asset in prosecution. I now think of the case of the NSA military sergeant who recently was reported in the press as having sold Top Secret information to foreign agents. Prosecution is stymied because of certain prosecutive prohibitions. Of course, thought could be given to putting this case on the "back burner" until these prohibitions are no longer valid and then resurrecting the prosecution so long as it still falls within the Statute of Limitations.

Finally, we must make a stronger effort to bring leakers to criminal justice or at least administrative justice so we can build a history of positive actions which will serve as a deterrent. To do this, all leak cases must be investigated aggressively. Military and other DoD components, since the abolishment of the Investigation Division of DINS in December 1972, have reportedly fallen back on the old "cop out" that "distribution has been too widespread for any investigation to be productive." Aggressive investigation in itself would make people within DoD, for example, aware of the Secretary of Defense's displeasure.

I hope that this statement will, if nothing else, convey the thought that to have tight security you must really want tight security and there be no exceptions. Otherwise all concerned are wasting their efforts.

There is no U.S. Government focal point for unauthorized disclosures within the Intelligence community. The FBI, for instance, only becomes aware of a disclosure when it is reported by a Government component or the White House orders it to investigate. Most disclosures are handled in-house. Within DoD military agencies, there is a built-in conflict of interests. No military agency will embarrass itself by identifying a high ranking individual as the source of classified matter. Only the former Directorate of Inspection Services had that capability.

Most important is that there is too much reluctance to declassify material appearing in the press to initiate an investigation. Military services, for example, tenaciously defend a classification which by its own downgrade stamp may have already dropped from Secret to Confidential, or even if it has already been declassified in an open hearing. Other prohibitions against declassifying may be valid for the time, allowing the culprit to escape prosecution rather than allow the U.S. to suffer national security damage, but never have I known anyone to monitor the case for further prosecution when the original prohibitions ceased to exist, bearing in mind the Statute of Limitations.

On occasion, an In Camera trial would be appropriate but our principal problem most frequently centers on the fact that the investigation is often aborted because of characters and "privileged leakers" (high Government officials and members of the U.S. House of Representatives and U.S. Senate) involved. Examples are provided in the Overt Leak section under the Discussion part.

Possible Solutions

Prosecution of leaks of classified data is generally considered under the Espionage Act, Sections 793 and 794, U.S. Code Title 18, and Section 2774, Title 42, U.S. Code of the Atomic Energy Act. These sections relate to "leaks" to the news media. In both instances punishment of the "leaker" can only be achieved if it is determined the person intended to injure the United States or provided data for the advantage of a foreign nation. Rarely can it be shown for criminal prosecution purposes that the "leaker" wanted to injure the United States. Yet it cannot be ignored that a "leaker" in causing such a disclosure to be made in the press has to be very naive not to know that enemy foreign agents are reviewing our newspapers and benefiting from the classified disclosures. Therefore, an appropriate amendment to Sections 793 and 794 and the Atomic Energy Act might be that it must be presupposed that in furnishing classified data which will appear in the press enemy foreign intelligence will become aware.

Discussion

Overt Leaks

No one could be more correct than the cartoon character, Pogo, to the effect that "We have met the enemy and they is us."

For many years there has been much concern over "leaks" of classified Defense information and there has been a great outcry about tightening the sections of the Espionage Statute which concerns itself with leak matter; promoting a British Official Secrets Act within the U.S. which shifts the burden of proof in some instances to the defendant as where a defendant is in receipt of classified information without authority; and to legislating an "In Camera" judicial procedure for holding a non-public trial involving the contents of classified documents, thereby precluding the need to declassify it for prosecution purposes, a current major stumbling block.

The practical side of the matter of curtailing "leaks" is that we wouldn't have very many if the investigatory process is allowed to proceed to the end which could result in criminal and/or administrative action taking place. For the greater part this doesn't happen because the investigation is often obstructed because of the characters and privileged leakers (high Government officials, Senators, Congressmen) who become involved and because of a dual standard of prosecution which exists. We always stand ready to take action against a GS-4 employee or a low ranking military person, but not against a high ranking person. Some examples of the above follow.

1. Neil Sheehan of The New York Times had published articles on Vietnam dated March 9 and 21, 1968. Both were referred to the FBI for prosecution. The classified data in the March 19 article came from CIA documents. Because the new Secretary of Defense, Clark Clifford, desired to have better relations with the press, the FBI was told that DoD had changed its mind about declassifying data in the March 21 article. Accordingly, when the CIA learned of this, it took the position that since DoD didn't want to go ahead with an investigation it would not pursue its case. The Assistant Attorney General therefore advised the FBI to cease its action. The March 19th article would have uncovered Daniel Ellsberg as its source. His identification would have spared us the Pentagon Papers, the Pentagon Plumbers, and all that followed including Watergate and President Nixon's resignation. Ellsberg confirmed he would have been trapped.

2. On March 26, 1970, an article entitled "Bunker in the Middle of the Chau Affair" appeared in the then Washington Star-News. Subsequent revelations revealed that the then Under Secretary of State, Elliot Richardson, was responsible for allowing Daniel Ellsberg to review highly classified cables and that Ellsberg subsequently leaked the data to the newspaper. The purpose reportedly was so that Richardson could focus President Nixon's attention on the plight of Tran Ngoc Chau, a Vietnamese assemblyman arrested by the Thieu regime. An investigation developed and the results were made known to Secretary of State William Rogers but the matter was never reported to the FBI and no action was taken against Ellsberg. It couldn't be without Richardson being accused also.

3. On May 23, 1969, an article appeared in the Washington Post entitled "Cost Study Urges Scuttling of Ten A-Subs," by George Wilson. The data was taken from a Secret memo entitled "FY 70 Budget" dated May 1, 1969. A bootlegged copy had been sent to Senator John C. Stennis' Senate Armed Services Committee. Subsequent investigation developed an excellent suspect. As the strings were being drawn tight, Senator Stennis contacted Secretary of Defense Melvin Laird and threatened if we did not cease our investigation he would initiate one on the Defense Department. Case Closed'.

4. On May 10, 1970, an article appeared in the Washington Post entitled "Secret Laird Memo Bans Any Talk Even Hinting ABM Halt is Desirable." A reference, but not a detailed article, appeared in The New York Times. The Post had totally published an April 22, 1970, Secretary of Defense, Melvin Laird, Secret-Sensitive memo, to all senior Pentagon officials and senior echelon military commands instructing DoD personnel not to carry on any discussion remotely suggesting a halt to the ABM (Anti-Ballistic Missile) Program was desirable. A copy of the Laird memo was furnished anonymously to the Washington Post and The New York Times newspapers. Subsequent investigation identified the culprit and the matter was referred to the Justice Department which had the FBI standing by to move in but Mr. Laird pulled the investigation back, claiming he made a deal with Tom Wicker of The New York Times that if he returned the copy of the memo in question, only "Administrative Action" would be taken. The Air Force Captain concerned was never directly accused and nothing was ever placed in either his Personnel file or Security file to reflect his deed. Had he come up for Major he would have been promoted.

5. The case breaking in December 1971 involving Yeoman Charles Radford and the transmittal of highly classified documents stolen from the briefcases of Dr. Henry Kissinger and General Alexander Haig was a classic case of an investigation being impeded by not only the White House but by Senator Stennis and his Senate Armed Services Committee. Although Radford confessed to purloining these documents, and his boss, Rear Admiral Thomas M. Welander, and Welander's boss, Admiral Thomas M. Moorer, admitted receipt of them, no action was taken. Senator Stennis' final report suggested that the actions of Radford and Welander should be considered in their next efficiency reports. Neither David Young or Egil Krogh (Co-Plumber Chiefs), myself (Chief Investigator of the DoD case), John Ehrlichman, or Jack Anderson was ever called by the Stennis Committee which held only 19-1/2 hours of hearings, including recess time covering 3-1/2 days over a 2-month period, and thereafter took 8 months to generate a ridiculous 11-page final report. The matter was never turned over to the Justice Department for a prosecutive opinion and the FBI was never requested to assume the investigation. It did piecemeal work, but never knew the full story.

6. On July 23, 1971, The New York Times carried an article entitled "U.S. Asks Soviets to Join in a Missile Moratorium," by William Beecher. Never have I seen the White House so shook up. President Nixon was furious because Beecher's article disclosed our fall-back position in the SALT discussions planned in the next day or two. Presidential tape conversations released of his July 27, 1971 conversations with Egil Krogh and John Ehrlichman demonstrated his wrath toward a then suspect, Dr. William Van Cleave. Again, this investigation met with obstruction. CIA [redacted] polygraphers were brought in sub-rosa and the FBI polygraphers were dropped at the last minute. Although the investigation led to the doorstep of Senator Henry Jackson, the FBI never was given authorization to interview him. Beecher, who was the subject of 22 investigations and, I believe, responsible for all principal SALT leaks from 1968 through 1973, was made Deputy Assistant Secretary of Defense in April 1973 and in September 1974 became Acting Assistant Secretary of Defense, departing in May 1975. Two months later he announced Top Secret information in an article in the Boston Globe dated July 31, 1975, entitled "U.S. Believes Israel Has More Than 10 Nuclear Weapons." Later a former DIA official confirmed Beecher's statement amidst refusals of comments from our State Department and the Israeli officials.

7. Briefly I'll refer to 3 separate cases involving Navy Admirals who were guilty of unauthorized disclosures, but only received a "slap on the wrist." One received an administrative transfer to Tokyo in 1967; another who compromised our 10-year lead over the Soviets on Anti-Submarine Warfare in 1969 received an oral reprimand. Senator or Congressman Chet Holifield, who was then head of, I believe, an Atomic Energy Committee, advised the Secretary of Defense by letter dated November 17, 1969 that he was satisfied with the oral reprimand and requested no written reprimand be placed in the Admiral's file. Dr. Foster, then Director of the Directorate for Defense Research and Engineering, was so incensed that he was ready to declassify necessary material for a prosecution; and lastly we have the Admiral who in April 1971 was strongly suspected of giving a Dr. Kissinger highly classified report to the president of an aircraft corporation and was allowed to "coast out" of the service into retirement a few months later unscathered although grounds existed for a prosecution.

8. Page 24 of Newsweek Magazine dated July 1, 1974, reflects a picture of Senator Lowell P. Weicker who admitted being the source of "key leaks in the early Watergate investigation." He stated he did it to promote the truth in the Watergate matter. Of course, there was no prosecution, not even a referral to Justice Department.

9. Congressman Michael Harrington in June 1975 admitted furnishing the press highly classified data about Central Intelligence Agency operations in Chile, causing great national security consequences. Chairman John J. Flynt of the House Ethics Committee dismissed the complaint against Congressman Harrington of unauthorized disclosure of a Secret CIA transcript because when the data was learned by Harrington it was not an official session of the House Armed Services Committee and no quorum was present. The case was never referred to the Justice Department.

10. And then there was the famous case of Daniel Shorr, who admitted he provided a House Intelligence Committee report to the newspaper Village Voice. Again this matter was never referred to the Justice Department, but instead the House Ethics Committee called in a team of former FBI agents to investigate, when the matter clearly fell within the FBI's jurisdiction.

11. And lastly we have Dr. Henry Kissinger's self-glorification leaks such as in the Edward R. F. Sheehan article entitled "How Kissinger Did It; Step by Step in the Middle East" and the hundreds of more White House, State Department and Military leaks to publicize the respective viewpoints and budget requests. Only the little person gets clobbered.

Categories of Leak Cases

1. Unauthorized disclosures in the news media may be said to fall in the following categories:

a. Those that appear in technical publications such as Aviation Week and Space Technology;

b. Those which are contrived leaks by someone in the administration;

c. Those which are leaked by the military to aid support of their budget request;

d. Those of a "if you can do it, I can do it" retaliatory nature when some high Government official, White House, or DoD, makes a statement utilizing classified information which he has just declassified, and a Congressman in defense of his position leaks something of a classified nature to support his point;

e. Those by an individual within the Government system who would have anti-war feelings or anti-U.S. Government feelings concerning dealings with another government;

f. Those of a nature where an individual in Government circles to impress a member of the press discloses wittingly or unwittingly his knowledge of a classified subject;

g. Those of a nature made by high level administration officials through impromptu replies to a newsman after a speech.

2. Explanation of the above:

a. Unauthorized disclosures appearing in technical publications frequently are determined to have been information which has been declassified previously as in the case of Congressional testimony, information of an unclassified nature which has been collated on a piece-by-piece basis and woven into an article; and information which public affairs departments of the contractor companies have released to get some "free publicity."

b. The contrived leaks are by individuals in the administration, who, in the case of SALT matters, released information as a trial balloon to get public reaction, to get Congressional support for defense appropriations sponsored by the administration, or to "do a little sword rattling" at the enemy.

c. Classified information leaked by the military to aid support of their budget comes at such time that there is an indication their request for additional ships, aircraft, or tanks may be cut off of a Defense appropriation. Some services even have their own favorite newspaper people to whom they provide the information.

d. "If you can do it, I can do it" cases developed from an administration official suddenly declassifying some material for the benefit of his argument being followed by a Congressman making his point indirectly through a news reporter by furnishing that individual classified information for a story to make his (Congressman's) point.

e. Those by an individual within the Government who opposed U.S. Government policy toward a foreign government arise from an individual's religious convictions or sympathy toward the foreign country, or his anti-war feelings.

f. Those of a nature where an individual in Government circles tries to impress the news media with the knowledge of how important he is and how much access he has to high level discussions and does so wittingly, and those where the individual makes unwitting disclosures to a news reporter by the news reporter's very clever questioning.

g. Those where a highly placed Government official handles so much classified material that he becomes oblivious to what is classified and what is not, and through questioning by news reporters after a speech makes an improper disclosure.

Covert Leaks

These are leaks of much greater importance as rule than Overt leaks as we only learn of them through informant coverage and often have no idea as to the full extent of the compromise. Unfortunately, as in the recent case of the Army Sargeant at NSA selling Top Secret data to foreign agents, the culprit may escape prosecution in the best interests of national defense. However, little thought, if any, has ever been given to consideration of resurrecting the prosecution later when the initial prohibiting factors no longer remain.

The sorry thing about the recent problem with the Army Sargeant is that we don't seem to learn anything from experience. In 1963, Army Sargeant Robert Lee Johnson, who was an NSA courier, was co-opted by the Soviets. In 1965, Air Force Sargeant Dunlap, also at NSA, was another Soviet conquest. All three of the above cases could have been avoided. Unless things have changed since I retired from the Government, the military services would not allow its personnel to be polygraphed, at NSA or elsewhere, yet routinely all civilian personnel were polygraphed. At one point and time it was my understanding that 50% of the military personnel who shipped over to civilian positions at NSA flunked out on the polygraph.

The normal procedure for the Soviets, after dealing with a co-opted U.S. person, is to polygraph him to check his integrity, but we don't feel it necessary to do the same for our own counterintelligence purposes. I would propose that all personnel holding sensitive intelligence positions be polygraphed at unannounced periods not to exceed one year. Such an action, had it been already in effect, would have undoubtedly surfaced the recent NSA Sargeant who foreign agents co-opted.

Potential Leaks

These are leaks which may result from some disenchanted person, military or civilian, defecting and orally providing classified information. Also, another source is from lost or misplaced classified documents. As regards disenchanted personnel, no mechanism exists for handling these people. It most often is done on a case-by-case basis by the agency or military service concerned with the highest emphasis being placed on avoiding embarrassment to their organization and lowest their concern for national security. The National Security Council (NSC) is rarely, if at all, informed. We are in need of an Intelligence Security Advisory Board, perhaps even as a part of NSC, to determine how these cases should be handled.

Examples of the foregoing are as follows:

1. In 1967 an Army enlisted man with Top Secret Communications knowledge deserted and while in neutral country indicated he intended to defect. The Army pleaded with him to return with the promise of an immediate discharge and no administrative action. This is the so-called commander's prerogative. He was returned and discharged at Ft. Dix, New Jersey. I personally called the FBI and arranged for him to be interviewed to determine his intentions.

2. In the middle 1960's there was a case [redacted] so highly sensitive it was assigned a code name. It involved an Army enlisted man possessing highly classified knowledge. He either contacted the Soviets or indicated he would. Initialy steps were taken to control him. Finally he was discharged from the military but contrary to popular opinion neither he nor the above-mentioned Army enlisted man, receiving the 24-hour discharge, came within the FBI jurisdiction, so the FBI could not monitor them. In the latter case a job was arranged for the discharged soldier but DIA (Defense Intelligence Agency) never bothered to keep a running damage assessment concerning his knowledge. No one seemed to know when his data would "cool." However, every time he disappeared DoD officials got quite excited.

3. Again in 1967 an ex-Air Force officer, who was a nuclear control officer abroad, became mentally unstable. He threatened to publicly disclose highly classified data. The Air Force promptly returned him to Andrews Air Force Base Hospital, gave him some psychiatric treatment, and then discharged him. I personally contacted FBI Headquarters and arranged to have him interviewed. He indicated he would return to Europe and go to East Germany. There was nothing the FBI could do; however, the Air Force, and the Army. as indicated above, each solved its problem by discharging the men.

4. In 1968 a Navy enlisted man contacted the Soviet Embassy in Tokyo and offered U.S. secrets. His commanding officer offered him immunity if he confessed, which he did. The Navy later assigned him to a distant post and kept him abroad until his enlistment expired.

In all of the above cases, the matters were all handled "off the top of the heads" of a few individuals and there was no coordination with interested Government agencies such as CIA and, in particular, the National Security Council. These cases surely indicate a need for more centralized control of such persons.

5. A case in point which, in my opinion, put personal embarrassment above national security is one concerning a high ranking civilian intelligence officer who was caught in a homosexual situation. This individual had access to a great deal of sensitive information and a compromise of him by enemy foreign intelligence could have grave consequences. The person in question was allowed to resign. Although my former office (DINS) was supposed to be notified of such situations, we were not. I was personally contacted by an irate intelligence officer in the man's organization. I was later told the person was very rank conscious and would not, if at all, be interviewed by persons of lesser rank. I believe I have a capability of bluntly expressing myself and I assured all concerned parties he would be interviewed or I would take personal action. It was imperative, and the concerned person knew it, that he be interviewed and polygraphed to assure us that he had not been co-opted by any enemy foreign intelligence because of his weakness. If so, much counter-intelligence action would have to be taken. The subject agreed to my request and our investigation reflected no compromise had occurred.

Numerous classified documents are lost. Normally only the losing agency is aware of the fact. No requirement exists to report same to anyone and most generally the matter is kept a secret. Even in those instances the documents are recovered, it is never known the extent to which a compromise may have taken place but at least some authority such as the National Security Council should be made aware.

One case which comes to mind took place in January of 1970 when the Top Secret Annual Report of Nuclear Stockpile Information sent to Ministers of Defense of NATO countries was, through sheer carelessness by an office in the Pentagon, distributed in the routine mail channels rather than by DIA courier. The Top Secret material sent to the Canadian Minister of Defense ended up being handled as though it was a piece of normal mail sent by any citizen, thereby being opened and reviewed at a very low level. Those reports sent abroad did not show up for at least 30 days, which brought the matter of possible compromise to our attention. We managed to track the mail from Washington to New York, by boat to Europe, and thereafter by train to certain foreign countries. In one instance we learned that the mail had traveled all through Yugoslavia and finally showed up in Athens, Greece. A military officer proudly informed me that the material had safely arrived and the envelope had not been opened. I then informed him that if the recipients in Greece could determine the envelope had not been penetrated, then I felt the whole Yugoslavia Intelligence should be abolished.

The important thing is that no mechanism or requirement then existed or now exists to alert the FBI, CIA, or the NSC. This can also be said for numerous other lost classified document cases. The other intelligence agencies could not take any positive action but, at least, could be alert through sources and informants for any information reflecting any knowledge of possible compromise.

Probably the most unique instance I know of concerning the Potential types relate to Yeoman Charles Radford and another sailor who worked in the National Security Council mailroom. When I came upon the latter as a possible accomplice of Radford's in connection with a 1971 military spying case on the White House, he was immediately transferred to his office of preference - Corpus Christi, Texas, where his wife, who refused to join him in Washington, resided.

Radford was a stranger to Admiral Elmo Zumwalt, who during the 1971-72 era was Chief of Naval Operations, but who had not been advised of the Pentagon spy matter involving Radford, Welander, and Moorer. It wasn't until January 4, 1972 that the then Acting Secretary of the Navy ordered Radford transferred "with no questions asked" as that, Zumwalt was told, was how the orders came from the White House. Zumwalt had to go to Admiral Moorer to learn of what had been going on during the two previous weeks. Initially Radford had been transferred to a billet in the Northwest which he did not like and made it known to Zumwalt. After much hassling, some two weeks later, Radford got the billet he desired. Zumwalt wasn't sure that he was, in fact, running the Navy or whether Radford was. Reportedly, the White House did not want Radford punished for fear he would testify in court about his spying activities on Kissinger and the President, and giving the results to Moorer.

In February of 1974, when Senator John C. Stennis of the Senate Armed Services Committee learned Radford would appear on the Mike Wallace "60 Minutes" Sunday night show, he quickly hi-jacked him by having the Navy deliver him to his office on the Saturday before his scheduled appearance. Radford appeared 10 days later before Stennis' Committee. Senate members of the Committee were heard to complain about getting the results of the Radford interview by Stennis when they arrived for the hearing on February 20, 1974, and not earlier when they might have prepared themselves to interrogate him on that day.

Transcript of the hearings reflect Radford was handled with "kid gloves," and the sailor in the NSC mailroom was never called to testify, and to my knowledge never interviewed under oath by the Committee or anyone else at any time.

The point of the foregoing is that the NSC mailroom sailor and Radford are still un-defused time bombs and still enjoy the status of the "Sacred White Cow of India." Each undoubtedly could embarrass the U.S. Navy and the U.S. Government.

In closing, let me say "leaks" of an Overt type can be greatly controlled if a more aggressive investigative effort is put forth. Leaks of the Covert and Potential type should be given more attention, and a greater effort to prosecute these cases and the Overt types should be made if there is to be any deterrent.

DDA 78-0551

DD/A Registry
File Legal-1

SENDER WILL CHECK CLASSIFICATION TOP AND BOTTOM

UNCLASSIFIED | CONFIDENTIAL | SECR

OFFICIAL ROUTING SLIP

TO	NAME AND ADDRESS	DATE	INITI
1	EO/DDA	2/9	
2			
3			
4	ADDA	10 FEB 1978	
5			
6	D/Security		

	ACTION		DIRECT REPLY		PREPARE REPLY
	APPROVAL		DISPATCH		RECOMMENDATION
	COMMENT		FILE		RETURN
	CONCURRENCE		INFORMATION		SIGNATURE

DDA 78-0551

Remarks:

FOLD HERE TO RETURN TO SENDER

FROM: NAME, ADDRESS AND PHONE NO.	DATE

UNCLASSIFIED | CONFIDENTIAL | SECRE

Distribution: (10 Feb 78)
1 - D/OS
1 - DDA Subject

	UNCLASSIFIED		CONFIDENTIAL		SECRET

EXECUTIVE SECRETARIAT

Routing Slip

TO:		ACTION	INFO	DATE	INITIAL
1	DCI		✓		
2	DDCI		✓		
3	D/DCI/IC				
4	DDS&T				
5	DDI				
6	DDA		✓		
7	DDO				
8	D/DCI/NI				
9	GC				
10	LC	✓			
11	IG				
12	Compt				
13	D/Pers				
14	D/S				
15	DTR				
16	A/DCI/PA				
17	AO/DCI				
18	C/IPS				
19	DCI/SS				
20					
21					
22					
	SUSPENSE	21 Feb 78			

[redacted]

ILLEGIB