AN ANALYSIS OF THE SYSTEMIC SECURITY WEAKNESSES OF THE U.S. NAVY FLEET BROADCASTING SYSTEM, 1967-1974, AS EXPLOITED BY CWO JOHN WALKER

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Military History

by

LAURA J. HEATH, MAJ, USA
M.S., Georgia Institute of Technology, 2001

Fort Leavenworth, Kansas
2005

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
17-06-2005	Thesis	Aug 2004 - Jun 2005

4. TITLE AND SUBTITLE

AN ANALYSIS OF THE SYSTEMIC SECURITY WEAKNESSES OF THE U.S. NAVY FLEET BROADCASTING SYSTEM, 1967-1974, AS EXPLOITED BY CWO JOHN WALKER

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Laura Heath

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
1 Reynolds Ave.
Ft. Leavenworth, KS 66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

CWO John Walker led one of the most devastating spy rings ever unmasked in the US. Along with his brother, son, and friend, he compromised US Navy cryptographic systems and classified information from 1967 to 1985. This research focuses on just one of the systems compromised by John Walker himself: the Fleet Broadcasting System (FBS) during the period 1967-1975, which was used to transmit all US Navy operational orders to ships at sea. Why was the communications security (COMSEC) system so completely defenseless against one rogue sailor, acting alone? The evidence shows that FBS was designed in such a way that it was effectively impossible to detect or prevent rogue insiders from compromising the system. Personnel investigations were cursory, frequently delayed, and based more on hunches than hard scientific criteria. Far too many people had access to the keys and sensitive materials, and the auditing methods were incapable, even in theory, of detecting illicit copying of classified materials. Responsibility for the security of the system was distributed between many different organizations, allowing numerous security gaps to develop. This has immediate implications for the design of future classified communications systems.

15. SUBJECT TERMS

Espionage, Walker spy ring, Fleet Broadcasting System, KW-7, Orestes system

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**		100	**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified	UU		

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Laura J. Heath

Thesis Title: An Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967-1974, as Exploited by CWO John Walker

Approved by:

_____, Thesis Committee Chair
Donald P. Wright, Ph.D.

_____, Member
Mr. Kendall D. Gott, M.A.

_____, Member
CDR Brett W. Wiseman, M.A.

Accepted this 17th day of June 2005 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

AN ANALYSIS OF THE SYSTEMIC SECURITY WEAKNESSES OF THE U.S. NAVY FLEET BROADCASTING SYSTEM, 1967-1974, AS EXPLOITED BY CWO JOHN WALKER, by MAJ Laura J. Heath, 99 pages.

CWO John Walker led one of the most devastating spy rings ever unmasked in the US. Along with his brother, son, and friend, he compromised US Navy cryptographic systems and classified information from 1967 to 1985. This research focuses on just one of the systems compromised by John Walker himself: the Fleet Broadcasting System (FBS) during the period 1967-1975, which was used to transmit all US Navy operational orders to ships at sea. Why was the communications security (COMSEC) system so completely defenseless against one rogue sailor, acting alone? The evidence shows that FBS was designed in such a way that it was effectively impossible to detect or prevent rogue insiders from compromising the system. Personnel investigations were cursory, frequently delayed, and based more on hunches than hard scientific criteria. Far too many people had access to the keys and sensitive materials, and the auditing methods were incapable, even in theory, of detecting illicit copying of classified materials. Responsibility for the security of the system was distributed between many different organizations, allowing numerous security gaps to develop. This has immediate implications for the design of future classified communications systems.

ACKNOWLEDGMENTS

I would like to thank my committee members for their support and good advice that was so critical to this thesis. I sincerely appreciate the time and effort provided.

TABLE OF CONTENTS

Page

ACRONYMS

CMS	Classified Materials System
DASD(C3I)	Deputy Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
DGDP	Directorate of Graduate Degree Programs
DIS	Defense Investigative Service
DoD	Department of Defense
DUSD(P)	Deputy Undersecretary of Defense for Policy
FBS	Fleet Broadcasting System
GDP	Graduate Degree Programs
KW-7	A type of encryptor used by the U.S. military, CIA, and allied nations during the 1960s, 1970s and 1980s. Also called the Orestes system.
NAVCAMS	Naval Communications Area Master Station
OSD	Office of the Secretary of Defense
PERSEREC	(Defense) Personnel Security Research Center

CHAPTER 1

INTRODUCTION

> Everyone makes a big deal out of the fact that I became a spy. It's because spying is such an unusual crime, but what they don't understand is that I became a spy because that is what I had access to. If I'd worked in a bank, I would have taken money. If I'd had access to dope, I would have sold drugs. The fact that I became a spy is really insignificant. The point is that I became a spy because I needed money. It was as simple as that.[1]
>
> John Walker, quoted in *Family of Spies*

CWO John Walker led one of the most devastating spy rings ever unmasked in the United States. Along with his brother Arthur, his son Michael, and his friend Jerry Whitworth, he compromised U.S. Navy cryptographic systems and classified information from 1967 to 1985--such a large quantity of information that, according to one report by a prominent Soviet defector, the KGB was forced to build an entirely new building to house all of the analysts working on it.[2] Despite the enormity of the compromises, however, the spy ring was caught only because John Walker's ex-wife turned him in to the FBI in a fit of drunken spite over unpaid hush money. That is, the communications security system in use was utterly unable to prevent or even detect enormously large-scale, long-term and devastating compromises.

Many people have asked the question, "Why did John Walker spy for the Soviets?" The answer is both amply documented and utterly simple: he was greedy. He wanted money, and he did not care whom he had to hurt to get it. Greed and selfishness are an unfortunate fact of human nature; there always have been, and always will be, pathologically greedy and selfish people in any organization as large as the U.S. Navy.

Given that this is well known to anyone who deals with human beings, a new question arises: since the presence of corrupt or corruptible insiders should have been a basic and obvious assumption, why was the communications security (COMSEC) system so completely defenseless against it? The purpose of this report is to answer that question.

To date, no unclassified study has been done to analyze the structure of the communications systems in use, to determine what design features failed (or were never implemented) which made them so vulnerable to an insider threat. A full accounting of the information that John Walker and his confederates compromised would be well beyond the scope of a report of this length. Accordingly, this research will focus on just one of the systems compromised by John Walker: the Fleet Broadcasting System (FBS), and further narrowed to focusing only on the period 1967-1974. It is a particularly instructive example for several reasons. First, FBS was the system used to transmit all U.S. Navy operational orders to ships at sea. This meant in practice that the full details of all U.S. Navy operations during the most intense fighting in the Vietnam conflict were transmitted using FBS and, consequently, were fully available to the Soviet Union while those operations were underway. Second, the cryptographic equipment used to secure FBS, called the KW-7, was the most widely used encryption device in the Western world, seeing service with all branches of the U.S. armed forces, other agencies of the U.S. government (such as the CIA and State Department), and many U.S. allies, such as North Atlantic Treaty Organization nations.[3] John Walker has confessed to giving the Soviet Union the complete technical specifications of the KW-7; this information, plus the fact that the Soviets are presumed to have obtained functional KW-7 encryptors from the USS *Pueblo* (seized by the North Koreans in January, 1968) and aircraft crash sites in North

Vietnam, would have allowed them to manufacture new KW-7 encryptors at will.[4] This means that the failure of the security measures taken for FBS also caused critical compromises in unrelated communications networks that used the same equipment. Lastly, focusing on the time period 1967-1974 is particularly illuminating because John Walker was working alone. This means that the security system failed when faced the simplest of all possible threats: a single, greedy sailor, working entirely alone. Looking at the simplest case gives the clearest possible view of the systemic weaknesses that resulted in the compromise.

Overview of the Thesis

This report, then, will look at FBS as a system, to analyze what was, or was not, done to take into account the unavoidable risk of rogue insiders betraying the secrets with which they are entrusted. The system had an elaborate and extensive security architecture. It was thought that numerous, overlapping security policies and procedures would make it much harder for a security breach to occur, because multiple, independent security subsystems would have to fail simultaneously for classified information to be compromised. This report will look in detail at three main areas of the security system and will show that in fact, there was no redundancy in the security design: a compromise in one area would lead to additional compromises in the other areas.

The first area to discuss is *personnel security*--policies and procedures which govern who is given (legitimate) access to classified information. They include how personnel are vetted prior to their first access to classified information, how they are monitored and revalidated during the period that they have access, and how their access is rescinded, either because they no longer need it to do their jobs or because of some

indicator of unreliability. In the case of John Walker, this is where the primary failure occurred. His case is an excellent, concrete demonstration of how poorly designed and executed the personnel security system was.

The second area to be studied is *technical security*--the security features designed into COMSEC devices (in this case, the KW-7 encryptor) that make recovering classified data from the transmitted message impossible for anyone except the legitimate recipient. The National Security Agency (NSA) was responsible for these technical security measures; by law, the NSA was solely responsible for design, testing, and manufacture of all COMSEC devices used by the U.S. government. Technical security is of critical importance because what the Soviet Union wanted most of all was a catastrophic failure of the technical security of the KW-7, which would allow them to decrypt any message that had been encrypted with a KW-7 as soon as it was received. CWO Walker was able to facilitate this primarily because he had easy access to the repair manuals and modification work orders for the device. This enabled the Soviets to reverse engineer new copies of the KW-7 whenever they wished, and to thoroughly examine the design for possible flaws.

The third security area to be studied is the issue of *key management*. A cryptographic key is a long random number that the encryptor uses to encrypt a message. (More details about how encryptors work are given below.) Cryptographic designers assume that the enemy will capture tactical encryptors eventually, such as by shooting down an aircraft that has one on board. Thus, they try to design and test their systems so that, even if the enemy has an identical encryptor, he will not be able to decrypt the data unless he also gets the key. Clearly, then, the distribution of the key is of primary

importance to the overall security of the system. All of the authorized recipients must have the correct key, or else they will not receive critical messages; but no unauthorized person can get the key, because this would allow them to decrypt secret messages if they do. These two imperatives conflict to some degree, and the issue calls for a delicate balancing of risks. Chapter four will cover the details of the key management system, and show how a highly insecure key management system was produced and used. It will show that the key distribution system, as actually implemented for FBS, was actually a substantial aid to John Walker in his espionage activities.

Another part of the key management system to consider is the auditing procedures used. Since it was known that the security of FBS depended on keeping the keys out of the wrong hands, there was a detailed and precise paperwork requirement at every stage of key handling. It gave the impression of being an extremely well thought-out, almost ironclad process. Yet obviously the audit procedures utterly failed to detect any compromise in this case. This report will examine why this was so, and will show that the audit and accounting procedures could not have caught any but the most naïve spy. CWO Walker was able to compromise almost every key that he touched between 1967 and 1974, yet the auditing system would not have been able to detect his espionage, even if every person in the audit chain had been 100 percent perfect in executing his duties.

This report will conclude with a chapter discussing the implications of the design and implementation problems of FBS. The KW-7 has long since been removed from the active inventory of cryptographic devices, but the lessons learned from this compromise have important implications for the design of current and future systems and for the risk analysis and management of classified materials. In particular, designers must take a

much more realistic view of the likelihood of insider malfeasance; indeed, they must assume that rogue users are present in every widely used communications or computer system, and design the other features of the system to detect and counter such users.

How do Encryptors Work?

Since this report will deal extensively with encryption systems, it is worth starting the discussion with a brief description of how machine encryption systems actually function. Concealing the meaning of a secret message depends on creating a *code,* or a systematic method of substituting random-appearing letters and numbers for the true secret message. The most common method used prior to the invention of machine encryptors was a codebook system. This required the sender to use pre-printed codebooks to look up each word in the secret message (called the *plain text*) and find its equivalent code word (called the *cipher text*). The receiver would have to look up each code word in the codebook and write down the equivalent plain text word.

For example, to encrypt the plain text message "Attack at dawn," the sender would look up "attack=MJWZJ," "at=RRVBX," and "dawn=PZAMQ" in his codebook. He would then transmit the cipher text "MJWZJ RRVBX PZAMQ." The receiver would use his copy of the codebook to look up "MJWZJ=attack," "RRVBX=at," and "PZAMQ=dawn" to get the correct plain text. *If* the code was properly designed and used, and *if* adversaries did not get a copy of the codebook, then the cipher text message was unintelligible. Using a codebook was slow and tedious, but it was effective for text messages sent by hand in Morse code.

Technology advances soon made manual codebooks impractical, however. Teletype machines could transmit hundreds or thousands of characters per minute,

making a manual lookup far too slow to be useful. Even more difficult was the case of pure data traffic, such as facsimile messages. How could a codebook be used to encrypt an image? However, the same technology advances that caused the problem also offered one possible solution. Consider the plain text message as simply a string of binary digits--ones and zeroes. Then suppose that, instead of a preprinted codebook with random-looking code words, both the sender and the receiver had the same, very long string of random-looking ones and zeroes to serve as a code. The sender prepares his plain text message, then lines it up digit-by-digit with his code. He then uses a simple substitution rule: if the plain text digit is the same as the code digit, he transmits a zero; if they are different, he transmits a one. Since the receiver has the identical string of code digits, he can reconstruct the plain text digit from the received cipher text; but to anyone without an identical copy of the code digits, the cipher text is unintelligible.

There remains the problem of ensuring that both the sender and the receiver have identical strings of code digits. The string of code digits must be as long as the message for this method to work--which meant billions of digits long, to handle a full day's data traffic at the transmission rates in use during 1967-1974. This meant that pre-positioning was a practical impossibility. Instead, cryptographic designers settled on a method called *key generation* to solve the problem. In this case, the human operator loads a single number, called the *key*, into the encryptor. The encryptor uses that number as a start point for iterating a complex mathematical formula to generate the string of code digits, also called the *keystream*. If the encryptor is properly designed, the resulting keystream will appear completely random to anyone who does not have the key--even someone who has the mathematical formula. Anyone who *does* have the key and the mathematical formula

embedded in the encryptor will be able to reproduce the keystream at will and will be able to easily decrypt the message.

The specific encryptor this report will examine was called the KW-7, or Orestes system. Physically, the KW-7 was a gray box, weighing about 75 pounds. It was based on a combination of vacuum-tube and transistor technology, and in 1967 it was the most widely used encryptor in the U.S. inventory.[5] To operate it, the radioman first had to key it, with a new key every 24 hours. Early models had a plugboard system, which required the operator to manually rewire a complicated pattern on a board on the front of the machine. For these machines, the key was the detailed wiring information, and it was delivered on a four-page booklet, containing six days worth of keying information. Later models were modified to take an IBM-type punchcard, with one key per punchcard.[6] The operator inserted the punchcard into a card reader on the front of the device to key it. The KW-7 was then ready to encrypt and decrypt messages.

Overview of the Fleet Broadcasting System

Establishing secure, reliable communications, both between ships at sea and ship-to-shore, has always been a major problem for navies worldwide. The development of effective high-frequency (also called short-wave) radios in the 1920s and 1930s produced a fundamental change in naval communications. These radios had ranges of hundreds or thousands of miles and allowed, for the first time in history, real-time coordination of naval action beyond line-of-sight. By the 1940s, voice and Morse code transmitters were being upstaged by radio teletypewriters and facsimile machines, enabling naval commanders to send extensive reports, and even charts and weather maps, around the

world in minutes. By 1947, the U.S. Navy was installing teletype and facsimile machines in every warship.[7]

During the period under study in this paper (1967-1974), the U.S. Navy's high-frequency radio-teletype system was the primary communications path. The main system for transmitting wartime information, orders, and status reports to, from, and between ships at sea was the Fleet Broadcast System (FBS). FBS has had many different configurations over the years; the design during this period had been implemented in 1964.[8] Every ship in the Navy had a teletype system that was capable of sending or receiving typed messages. The teletypewriter connected to the KW-7 encryptor, which automatically encrypted messages before transmission and decrypted messages on receipt.

The Navy's high-frequency radios had a long range, but not long enough to circle the globe. Accordingly, the world was divided into four theaters (Eastern Pacific, Western Pacific, Atlantic, and Mediterranean), each with one Naval Communications Area Master Station (NAVCAMS).[9] The NAVCAMS was responsible for all communications in its area and for supporting all ships operating (or transiting through) there. The NAVCAMS was also responsible for maintaining all of the keying material used on its networks and for ensuring that all ships received copies of the keys that they would need prior to entering its area. John Walker began his spying activities when he was given access to the master key vault for the submarine forces, Atlantic command (CINCSUBLANT) and over the course of the following seven years managed to compromise key material from all four NAVCAMs at some point.

Overview of the John Walker Spy Case

John Walker was born on 28 July 1937, the second son of James and Peggy Walker. His home life was tempestuous, to say the least; his father was a violent alcoholic who eventually drove the family to bankruptcy and then abandoned them. As an adolescent, John Walker became first a troublemaker, then a petty criminal. When he was 17, he was finally caught by the police for burglarizing a gas station and a men's clothing store, after a high-speed chase through town. His older brother, Arthur Walker, had joined the Navy directly out of high school, and intervened to convince the judge to allow John to join the Navy also. It was common enough at the time to solve the problem of a disruptive young man by forcing him into the military. The general thought that military would straighten him out and give him discipline and direction in his life.[10]

That certainly seemed to be the case for John Walker. He entered the Navy in 1956, as a Radioman, and seemed to thrive. There was no record of discipline problems, and he made a very favorable impression on his superiors. He made rank quickly, achieving a rating of RM1 (E-6) in only six years, and his evaluation reports were almost perfect (4.0) ratings.[11] He got his girlfriend, Barbara Crowley, pregnant, but he "did the right thing" and married her in 1957. They had their first child, Margaret Ann, that same year, and a second daughter, Laura, followed in early 1960. He volunteered for submarine duty, on the recommendation of his brother Arthur (who was also a submariner), and in June 1960 he was accepted for submarine training, followed by an assignment to the USS *Razorback* (SS-394), a World War II-era diesel submarine based in San Diego, CA. In 1962, he was reassigned to the newly commissioned USS *Andrew Jackson* (SSBN-619), one of the first nuclear-powered ballistic missile submarines, home

ported in Charleston, SC.[12] On the surface, then, John Walker seemed to have put his dodgy past behind him and grown up to be a responsible petty officer and family man. Digging a little deeper reveals a much different situation. While his duty performance remained high, his home life was growing ever more acrimonious. Both John and Barbara Walker were drinking heavily, and John Walker was spending more and more of his time carousing with his fellow sailors rather than home with his family.

He was first submitted for a Top Secret clearance while he was assigned to the USS *Andrew Jackson*, and it was granted without comment on 29 December 1964. The following year, he was promoted to chief petty officer and reassigned to the USS *Simon Bolivar* (SSBN-641), a newly commissioned nuclear ballistic missile submarine also home ported in Charleston, SC. In 1966, he was promoted to warrant officer. That same year, he decided to start a business of his own. He thought a bar and snack shop would be a sure-fire winner near a Navy base and so took out over $20,000 in loans to set up the Bamboo Snack Bar. Unfortunately for him, the business lost money the entire time it was open. By 1967, the Walkers were on the verge of bankruptcy, adding the stress of financial difficulty to the already highly dysfunctional atmosphere at home.[13]

In November, 1967, John Walker was reassigned as a watch officer in the submarine fleet message center, NAVCAMS, Atlantic fleet, at Norfolk naval base. Barbara Walker and the children remained behind in South Carolina, to run the Bamboo Snack Bar. Quite unexpectedly, in December 1967, he returned with several hundred dollars in cash, plus Christmas gifts, and more money to pay off some of the most critical overdue loans. He claimed he had gotten a second job, but Barbara Walker did not believe him--she assumed he was into some sort of criminal activity. She was even more

suspicious when the family joined him in Norfolk in 1968. She discovered that he had rented a luxurious apartment, and together they spent over $10,000 in cash on new furnishings. While snooping around the apartment, she found a set of instructions for delivering classified materials to his handlers; when she confronted John Walker with this evidence, he confessed to her that he was spying for the Soviet Union. He claimed they were paying him $4,000 a month, plus bonuses, for stealing secrets from the NAVCAMS vaults. (For comparison, his legitimate salary as a warrant officer was $725 a month.)[14]

Although the money was good, he was feeling highly stressed about his espionage. He later testified that he felt like he was in constant danger from the FBI while he was so near Washington, D.C. The stress was also taking its toll on his duty performance; in fact, the period 1968-1969 was the only time in his career where his duty ratings were less than excellent. He was convinced that his supervisors were beginning to get suspicious of him. Interestingly, that was not true. His supervisors thought he was careless, obnoxious smart-aleck, and they held him in contempt for his open womanizing, but they apparently never considered the fact that he might by selling secrets.[15]

Nonetheless, he decided to ask for a transfer away from Norfolk in mid-1969 and was reassigned as an instructor at the radioman school in San Diego, California. During this assignment, he realized that it would be less risky for him if he could recruit someone else to do the actual spying and serve instead as a go-between or spymaster. He carefully probed his students for weaknesses, and would eventually recruit one of them, Jerry Whitworth, to spy for him after his retirement in 1974. He also realized that he needed the Soviets' money. They had cut his "salary" in half, to $2,000 a month, because he no longer had access to key materials. That proved to be too little for John Walker to carry

on the lavish lifestyle he had become accustomed to, and so he volunteered to transfer to a sea duty billet to gain access to a COMSEC vault again.[16]

In late 1971, he was reassigned to the USS *Niagara Falls* (AFS-3), a resupply ship based in Oakland, CA, but due to sail in support of operations off the coast of Vietnam shortly. He was given the position of Classified Material System (CMS) custodian, which gave him full access to all cryptographic and classified material onboard. While off the coast of Vietnam, he repeatedly volunteered to serve as a courier for classified materials, both between Navy ships and between shore bases and ships--primarily because the Soviets were paying him a "bonus" if he could get additional classified information.[17]

He had been hiding the cash that the Soviets were paying him in a can, buried under one corner of his garage. When he returned from his Vietnam deployment, he found out that his family had discovered the location of his stash and spent all the money. He was flat broke. It was the last straw for him, and he filed for divorce from his wife. He told her that, if she stayed quiet about his spying, he would pay her an extra $1,000 a month in "alimony," above the $500 a month that the court ordered in child support. (His legitimate salary was only $18,000 a year, so the amount he was offering was 100 percent of his total legitimate income.) He also realized that Barbara Walker, embittered and alcoholic, was hinting to people around her that he was spying, and he decided that he had to get out of the Navy to protect himself. He spent the last two years of his career supervising the distribution of classified material in Norfolk, VA, and then retired on 31 July 1976.[18]

After his retirement, he was nominally working as a private investigator in the Norfolk, VA area. In fact, most of his income came from running a spy ring that grew to include his former student Jerry Whitworth, his brother Arthur Walker, and his son Michael Walker. And it was this recruitment of his family members that, ironically, led to his capture. Barbara Walker reported him to the local FBI office in Hyannis, MA, in November 1984 because he had stopped paying her the agreed-on hush money, and because she was outraged that he had tried to recruit their daughter, Laura Walker, and Laura Walker's ex-husband was using this fact to blackmail her to prevent her from getting custody of their son. The FBI agent who interviewed her thought that she was drunk and rambling, and that she was making up a story to get revenge on an ex-husband; nevertheless, since the crime was alleged to have taken place in Norfolk, the report was forwarded to the Norfolk FBI office for final disposition--with a recommendation that it simply be closed and filed. The report went to Special Agent (SA) Robert Hunter, who was in charge of espionage cases at that office. He thought that the story rang true, somehow, and he began some preliminary investigation to see if some of the details might be corroborated. Somewhat to everyone's surprise, the details did check out, and the investigation began to gain momentum. After months of painstaking work, the FBI managed to catch John Walker in the act of leaving a bag containing 129 classified documents, disguised as a bag of trash, by the side of the road for pickup by a KGB officer assigned to the Soviet Union's Washington, DC embassy.[19]

---

[1]Pete Early, *Family of Spies: Inside the John Walker Spy Ring* (New York: Bantam Books, 1988), 14.

[2]Testimony of Vitaly Yurchenko, cited in Robert W. Hunter and Lynn Dean Hunter, *Spy Hunter: Inside the FBI Investigation of the Walter Espionage Case*

(Annapolis, Maryland: Naval Institute Press, 1999), 202. It is worth mentioning that there are some remaining doubts about Yurchenko's testimony. He defected in 1986, after the public announcement of Walker's arrest but before his trial, and seemed very eager to credit the Walker ring virtually all of the Soviet Union's intelligence successes. Yurchenko subsequently snuck away from his FBI handler and returned to the Soviet Union, claiming that he had been kidnapped by the US government. Some agents believed that his "defection" was simply a KGB ruse. Following this line of reasoning, the KGB knew that Walker would talk, even brag, about his spying; hence, he could be a convenient scapegoat for information leaks that in reality came from other Americans then actively spying for the USSR, such as Aldrich Ames and Robert Hansen. This particular fact, however, is probably true; this report will show that the Soviet Union was decrypting hundreds of thousands, possibly millions, of classified messages yearly due to the Walker spy ring's activities.

[3]Jerry Proc, "KW-7" (date unavailable), http://www.jproc.ca/crypto/kw7.html (13 January 2005).

[4]Early, 72.

[5]Proc, "KW-7"

[6]Testimony of John Walker in *U.S.A. vs. Jerry Alfred Whitworth* (U.S. District Court, District of Northern California, Case No. 85-552, vol. 24), 24-2817.

[7] Office of the Chief of Naval Operations, *U.S. Naval Communications Chronological History*, 1961.

[8]OPNAV Report 5750-5, *History of the US Naval Communications Center Norfolk, 1 January 1965-31 December 1965*, pp. 28-31.

[9]Early, 58.

[10]Pete Early, *Family of Spies: Inside the John Walker Spy Ring* (New York: Bantam Books, 1988), 20-34, and Pete Early, "Court TV's Crime Library, Criminal Minds and Methods: The John Walker Spy Ring" page 2 (date unavailable), available at http://www.crimelibrary.com/terrorists_spies/spies/walker/2.html?sect=23; Internet.

[11]Robert W. Hunter and Lynn Dean Hunter, *Spy Hunter: Inside the FBI Investigation of the Walter Espionage Case* (Annapolis, Maryland: Naval Institute Press, 1999), 25-26.

[12]Early, 34-43.

[13]Ibid., 52-57.

[14]Ibid., 58 and 63-74.

[15]Ibid., 78-81.

[16]Ibid., 84-97.

[17]Ibid., 98-108.

[18]Ibid., 108-143.

[19]Hunter, 3-71.

CHAPTER 2

PERSONNEL SECURITY

> CWO-2 Walker is intensely loyal, taking great pride in himself and the naval service, fiercely supporting its principles and traditions. He possesses a fine sense of personal honor and integrity, coupled with a great sense of humor. He is friendly, intelligent and possesses the ability to work in close harmony with others. He is especially at ease in social situations and has an active self-improvement program which includes enrollment in the commercial instrument flying course and the completion of naval intelligence correspondence course. He is an active sailboat enthusiast and an accomplished aircraft pilot...[1]
>
> John Walker's 1972 fitness report, quoted in *Family of Spies*

Personnel Security Overview

Personnel security is an overarching term for the collection of laws, policies and procedures that attempt to ensure that only trustworthy persons get access to classified information. Clearly, this is fundamentally important to preventing enemies from getting access to classified information. It is arguably the most difficult part of the security system to get right. Human beings are inherently complex, even contradictory, and have a wide range of possible motivations for their actions. Policy has to be written that takes into account what people might do when driven by impulse, malice, greed or fear, yet not compromise the rights of innocent citizens or overburden the administrative system. In fact, even that is not enough; well-intentioned people can compromise data through ignorance, carelessness or the immediate pressure to accomplish a mission, and the policy must take that into account as well. Lastly, policy must be implemented--primarily by personnel who were selected, rewarded and promoted for their success as *sailors*, not as security experts. When inevitable conflicts arise between the demands of security policy

and mission accomplishment, the personnel who will have to resolve the dilemma will be primarily focused on mission requirements and may not have a clear idea of what the security implications of their actions are.

The sheer number of persons to be evaluated for trustworthiness and reliability was daunting. The Stilwell commission, looking at the Department of Defense in 1985, found that almost four million people needed access to classified information to do their jobs. More than three million people held current Secret or Top Secret clearances, and almost one million new Secret or Top Secret clearance requests were submitted every year.[2] Attempting to write a single set of policies and procedures that would identify the possible security risks from such a large pool of people is clearly a major challenge.

Amazingly, no one had actually attempted to do such a comprehensive analysis of threats, risk, operational needs, and resources available. Personnel security policies in the U.S. Navy were based on a variety of sources, including federal laws, executive orders, and directives from the Secretary of Defense, Secretary of the Navy, and the Navy chain of command. Most of these laws and orders were enacted to remedy specific vulnerabilities (often after compromises had been discovered) rather than to create or implement an overarching system. No single person or office had control, final approval authority, or even complete knowledge of, personnel security policy. Within DoD, responsibility for developing security policy was divided between the Deputy Undersecretary of Defense for Policy (DUSD(P)) and the Deputy Assistant Secretary of Defense for Command, Control, Communications and Intelligence (DASC(C3I)); both the DoD Inspector General and the DoD General Counsel also had statutory oversight roles. Other policy was also written by the Director of Central Intelligence and the Office

of Personnel Management, which affected DoD personnel working on some, but not all, classified programs.[3] The DUSD(P) had a Directorate of Counterintelligence and Security Policy; with a staff of just 25 personnel, it was responsible for writing policy and overseeing its implementation in areas as diverse as personnel security, information security, physical security, release of classified information to foreign governments, industrial security, special access programs, operations security, counterintelligence and more. There was no formal process for staffing changes to regulations and directives among these disparate organizations, and there were no clear instructions on what to do if different directives conflicted.[4]

The personnel security system that resulted from this mish-mash of directives had three main components. First, it sought to ensure that only reliable and trustworthy persons were granted access to classified information by investigating applicants' background and bona fides prior to granting security clearances. For high-level security clearances, personnel were supposed to be re-investigated on a periodic basis as well. Second, both supervisors and co-workers were expected to report behavior that indicated a security risk or personal unreliability. Lastly, professional law-enforcement and counterintelligence agents were charged with investigating possible espionage and prosecuting those who were guilty. John Walker had little trouble bypassing all three elements of this system.

Granting Initial Secret Clearances

Security clearance requests are initiated by the organization where the nominee works, and are supposed to be requested only if the nominee requires access to classified information to perform his mission. The nominee would fill out a personal history

statement, and his unit would then forward it to the Defense Investigative Service (DIS) for a background investigation and granting of a clearance. For a Secret clearance, the investigation consisted entirely of a National Agencies Check (NAC), which looks for the nominee in the FBI's criminal record database and the Defense Central Index of Investigations. This check would only show federal convictions or previous investigations by the Department of Defense; state and local offenses, even felonies, would not appear. If the nominee did not volunteer the information on his personal history statement, it would not be found.[5] Since the great majority of criminal investigation and prosecution is done at the state or local level, the NAC was almost useless for its stated purpose of preventing criminals from gaining Secret security clearances. There was no attempt at all to identify personnel who had any noncriminal indicators of potential security weakness, such as a history of mental illness or financial difficulties.

John Walker is an excellent example of the limitations of such a cursory investigation. He entered the Navy in 1955, after being arrested for a string of ten break-ins and burglaries, culminating in a high-speed chase and shots fired at a policeman.[6] He confessed and was convicted, but the judge reduced his sentence to probation, due to the fact that he had no previous record and was only seventeen years old at the time of the crimes.[7] His brother, Arthur Walker, who was a Navy petty officer at the time, came home on leave and decided that the Navy could straighten him up. As Arthur Walker tells the story:

> We walked in [to the recruiter] and I was in my Navy blues and I said, "I got my brother here and he wants to join up," and this recruiter starts going crazy because he is so happy. Well, John went through the basic questions and when the

> recruiter came to the one about having committed any criminal acts, John said that he had been arrested and the recruiter slowed down a bit, and then the recruiter says, "What did you do?" and John tells him, and this guy flips out and says, "Sorry, we can't take you unless you get the judge to lift your probation." So John and I walked across the street to the courthouse and went up and I found the judge and said, "Your Honor, my brother wants to join the Navy and I think it would really help him out." Well, we talked for a while and the judge agreed and called the recruiter, and the next think you know, John is in the Navy. I went back to submarine duty and John went off to boot camp.[8]

John Walker was given the rating of Radioman, and a Secret clearance, the following year.[9] There are two things to note about this incident. First, notice that, although John Walker had a proven history of antisocial behavior, it was impossible for the people who made the decision to give him a Secret clearance to know about it. He was convicted under state law, not federal, and so the NAC would not reveal the misconduct. He had also been convicted as a minor, which meant that his records were sealed. In many states, juvenile court records were not released to anyone, including federal investigators, without a warrant.[10] Second, notice that it was clearly against stated policy for John Walker to join the Navy in *any* capacity. He was able to enlist because four people--his recruiter, the judge, his brother, and he himself--colluded to keep the information about his criminal behavior out of official files. Their motivations to do so varied considerably. The recruiter was rewarded for enlisting new sailors, not for turning potential recruits away. If John Walker could be brought from just below to just above the minimum requirements for enlistment, then the recruiter was happy to help make that happen. The judge was interested in removing a juvenile delinquent from his community. Forcing someone to join the military was a fairly common way of dealing with troublesome, disruptive young men in those days, and the judge probably thought that it was an easy way to make a problem go away. Arthur Walker, on the other hand, was motivated by

concern both for his brother and for the rest of his family. He thought that the Navy would be able to give his brother the discipline and maturity that he so desperately needed, and in so doing would stop him from causing further pain to his family. And lastly, John Walker himself was simply looking for a way out of a jam. He had discovered that his criminal record made him essentially unemployable in his home town, and he was looking for a fresh start and a new place to live.

In short, the U.S. Navy had a screening system in place to prevent people like John Walker from entering military service or being granted access to Secret information. However, that system's effectiveness depended on the people involved with the system actively assisting in the discovery of derogatory information and the denial of security clearances. That was a highly unrealistic assumption, for two main reasons. First, many of the people who were responsible for protecting the Navy from criminal entrants were not themselves members of the Navy--the applicants themselves, judges, law enforcement personnel, and so on--who could not reasonably be expected to have any loyalty toward the Navy or even any knowledge of its regulations. Second, the system rewarded the concealment and punished the revelation of derogatory information on applicants. It is almost as if the system was perversely designed to *not* find derogatory information on applicants for a Secret clearance. This combination of skewed rewards and dependence on the altruism of strangers produced a system that allowed John Walker to easily gain access to the nation's secrets.

Granting Initial Top Secret Clearances

Obtaining a Top Secret clearance was a much more thorough process. The most notable change was that clearances required a field investigation by the Defense

Investigative Service (DIS)--that is, a professional investigator would conduct interviews to verify the nominee's bona fides and look for indicators of unreliability.[11] The results of the investigation would be forwarded to an adjudicator, who would determine if the nominee should or should not be granted a clearance. There was an additional layer of oversight, called the crypto access program, for personnel (like John Walker) who had highly sensitive or long-term access to cryptographic devices or materials. Persons in the crypto access program were to be identified and specially managed by the personnel system; some billets were restricted to only those sailors enrolled in the program.

These safeguards would seem to be a solid defense against unreliable personnel getting access to classified material. Yet the John Walker case gives some excellent examples of how troubled the system was. He was first nominated for a Top Secret clearance in 1962. The investigator did know about his juvenile conviction, and in fact was able to read the sealed court records; however, he thought that it was just one incident (rather than ten or more). Furthermore, John Walker had been in the Navy for nine years at that point, and his file showed a consistently outstanding level of performance.[12] He had been promoted very quickly, rising to Petty Officer 1st Class in only six years and Chief Petty Officer in only nine.[13] By 1962, he was married and had three children, and to the investigator, it seemed that he had put his youthful indiscretions behind him. He would hardly have been the first troubled young man to have been straightened out by the Navy. The investigator asked his neighbors and references questions about whether he might be homosexual, an alcoholic or drug user, whether he had financial troubles, and whether he had any contacts with foreigners. No one raised

any red flags, and the investigator recommended granting him a TS-Crypto clearance. He was granted Top Secret/Crypto access clearance on 29 December 1964.[14]

Yet red flags there should have been. According to Donald Clevenger, one of John Walker's shipmates, "I think all of us had a drinking problem during those years. Our life-styles were built around parties and booze. There always seemed to be a group of people at Johnny's house, a special gang. Usually they were radio people from the boat."[15] John Walker's wife was also an alcoholic, and their marriage was obviously troubled. In one particularly vivid example, when Barbara Walker went into labor with their third child, John Walker dropped her off at the hospital and then went to a softball game with his shipmates. He had also been involved in a string of more-or-less open extramarital affairs and liaisons with prostitutes.[16] All of this was done in plain sight of his shipmates and friends, yet no one mentioned a thing to the investigator.

One lesson to draw from this episode is that people look at and report on a co-worker's behavior relative to the culture and command climate in their immediate work area. As seen in Mr. Clevenger's comments above, the radio section of John Walker's submarine was comprised in large part of heavy drinkers. Alcohol binging was a considered normal and expected way to relieve stress and enjoy time off, and even outright alcohol abuse carried little social stigma. Arguably, the Navy culture of the time was so strongly pervaded with heavy alcohol use that he would have been more suspicious looking to his shipmates if he had been a teetotaler than an alcoholic. Likewise, extramarital affairs and open involvement with prostitutes were tolerated, at least for enlisted sailors during port calls overseas. Certainly, John Walker never felt the

need to hide his behavior--quite the contrary, he often invited his shipmates along--nor did he ever face negative consequences of any kind for moral turpitude.

A thornier issue is the question of what characteristics or behaviors actually represent an increased risk of security compromise. Clearly, the decision to grant or withhold access to classified materials should depend on how likely the applicant is to mishandle those materials. Yet in 1985 the Stilwell Commission found that there was little or no empirical evidence available for adjudicators to use when making their decisions; there was also no formal training or certification program in place for adjudicators either. Adjudicators were told simply to use their "overall common sense" and, if it was "not clearly inconsistent" with national security, to grant access to the individual. This standard was so hazy that different adjudicators could easily come to different conclusions about whether to grant access, even based on identical facts. Some adjudicators would apparently grant access to almost anyone; overall, the rejection rate was only about 2.5 percent, and for contractors the rate was a miniscule 0.2 percent.[17] To further muddy the waters, the U.S. Navy treated the adjudicator's decision as merely advice to the applicant's commanding officer. Commanders could grant or deny access to Top Secret information to sailors under their command irregardless of the results of the investigation--or even irregardless of whether any investigation had been done at all. Yet these commanders had no training at all on the wider implications of granting access to individuals without vetting them thoroughly.[18]

As an example of this, consider the question of heavy alcohol use. It may seem obvious common sense that a heavy drinker is a higher security risk than a nondrinker. Yet hard statistical evidence about how much alcohol affects a person's reliability was

sorely lacking. How much alcohol consumption indicates an increase in the risk of mishandling classified material? One drink a week? One a day? Six a day? Is a binge drinker worse than a steady drinker? What should be the cutoff, and how will the relevant information be discovered? It may seem "obvious" that a heavy drinker is likely to be unreliable, but many sailors who served with John Walker were heavy drinkers, yet espionage was literally unthinkable to anyone but him. Likewise, it would be very hard to characterize John Walker's espionage as related to his alcohol use. As matters stood in 1965, the only information about an applicant's alcohol use that would appear in his file would be whether or not his neighbors and co-workers thought he had a problem with alcohol. All this really showed was whether the applicant was more-or-less congruent with the current social mores in his small circle of acquaintances, rather than any objective standard of alcohol abuse or dependence. Then, the individual adjudicator made a personal, "common sense" decision about how "bad" the reported alcohol use was, and he recommended either for or against granting the applicant a Top Secret clearance. This was subject to being overridden by the applicant's commanding officer, again based solely on individual "common sense" about the security risks. Clearly, this is not a rigorous and fair method for evaluating potential espionage threats.

An even better example of the weakness of the security investigations is the question of homosexuality. In 1965, when John Walker was investigated for his Top Secret clearance, homosexual orientation was categorized as a mental illness, and homosexual behavior was both illegal and grounds for immediate dismissal from the service. By the "common sense test" of the time, it was an obvious disqualification for holding a security clearance. Following a notorious espionage case at the National

Security Agency (NSA) in 1960 that involved two homosexual employees defecting to the Soviet Union, every security investigation included an explicit evaluation of whether the applicant might be homosexual.[19] John Walker's investigation dutifully noted that he was not.[20] Yet over the years, society's opinions about homosexuality underwent radical changes. The American Psychiatric Association removed homosexuality from its list of mental illnesses in 1973; instead, it announced that, "homosexuality, per se, implies no impairment in judgment, stability, reliability, or general social or vocational capabilities."[21] Over the next twenty years, through a series of court cases, executive orders, and guidelines memoranda, homosexuality policy was completely reversed: instead of requiring investigators to determine an applicant's sexual orientation and denying security clearances to homosexuals, they were *forbidden* from asking about sexual orientation and from using homosexual orientation as a basis to deny a clearance.[22] Note, however, that neither the original policy nor any of the subsequent changes were based on any empirical knowledge of whether homosexual behavior changed the likelihood of the applicant mishandling classified materials. When homosexuality was considered "sexual deviance," it was considered an obvious reason to deny someone a clearance; no proof of this assumption was ever offered, or even sought. Likewise, the changes were introduced as civil rights and antidiscrimination measures, rather than in response to empirical evidence that homosexual behavior is irrelevant to security reliability. This is one more example of security imperatives being subordinated to other obligations.

Reinvestigations

The regulations also called for reinvestigating Top Secret clearance holders every five years. It was known that, in principle, reinvestigations are more important than initial investigations. This is because almost all spies are recruited *after* they get access to classified material; very few initially apply for access intending to spy.[23] In the case of John Walker, the first thing that the Soviets asked him to bring them was not classified or cryptographic material at all--it was the names and biographies of everyone else working in the communications center, plus any information about possible personal weaknesses that the Soviets could exploit.[24] In other words, the Soviets' first priority was to develop new spies, rather than to obtain classified material directly--even though John Walker was able to give them extremely sensitive and valuable data. Yet in practice, conducting initial investigations always took precedence over periodic reinvestigations when time or resources were tight. It is not hard to see why. Sailors who were awaiting the results of their initial clearance were unable to work in their intended jobs, which meant that the radio or cryptographic section was short handed, while a "perfectly good" sailor twiddled his thumbs. Sailors who were due a reinvestigation were allowed to continue working; they were seen as "proven" trustworthy, and the reinvestigation was seen as simply an administrative chore that some other organization was responsible for.

In John Walker's case, he should have been due a five-year reinvestigation in late 1969. He started spying at the end of 1967, and by 1969 he was living very conspicuously beyond his means. His Navy salary as a warrant officer was $120 a week; the Soviets had been paying him $4,000 a month, plus substantial bonuses for specific items, since January 1968.[25] However, DIS was so seriously backlogged on the initial investigations

that reinvestigations were suspended entirely for several years. John Walker did not come up for a periodic reinvestigation until 1972.

He expected to fail the reinvestigation. He had been spending almost ten times his yearly salary for five years, routinely abused alcohol and marijuana, had a series of blatant extra-marital affairs (including taking his mistresses to the Officer's Club on post), and his wife, who was also an alcoholic, had been complaining to her friends and co-workers about his spying, among other indicators of trouble.[26] His solution was ingenious: he stole his own personnel records, plus the records of another sailor who had just completed a periodic reinvestigation. He found that the proof of a completed reinvestigation was simply a one page form which had been stamped with the FBI seal. He carefully copied the seal onto tracing paper, then took the traced design to a local print shop to have a duplicate stamp made. (He went in uniform and implied that he needed it for official business.) He stole a blank form from the ship's stores, forged a completed reinvestigation form on himself, and replaced the stolen files. John Walker bragged later that it cost him less than $3 to fool the security officer into thinking that he had already been submitted and cleared on the reinvestigation.[27]

This is a clear indication that the security reinvestigation process was seen as just an administrative chore, rather than a critical piece of the overall security system. The forms involved were treated just like any other personnel form--kept in an unlocked file cabinet, easily available to anyone who might want one. Sailors had access both to their own files and other sailors' files, and there was no means of determining if anything had been added to or subtracted from the file. The verification process was such a minor issue that no one expected the officer in charge to remember whether he had submitted a

particular sailor or not. The proof of a completed investigation was a rubber stamp on a piece of paper--a trivial thing to counterfeit.

All in all, the system treated reinvestigation in an almost shockingly casual way. It stands in dramatic contrast to areas where the Navy took administrative requirements seriously--such as training and certification requirements for pilots. For example, it simply beggars belief that a Navy pilot would have been allowed to fly for three years without a current flight physical, because the medical system was backlogged. The Navy understood that naval aviation was a vital part of modern naval operations, but that it carried with it the inherent chance for catastrophic disaster. To minimize that chance, the Navy invested huge amounts of time and effort in ensuring that pilots were fully trained, carefully monitored and evaluated throughout their careers, and removed from duty if their behavior or skills warranted it. Nevertheless there is no evidence that the Navy, as an institution, ever realized that the same facts were true about its high-speed digital communications networks--they were indispensable to modern naval operations, but they could cause catastrophic disaster if penetrated. As a consequence, the investigation and reinvestigation portion of the personnel security system was never resourced adequately, and when personnel security requirements were seen as too burdensome, they were ignored.

Reporting and Acting on Suspicious Behavior

The personnel system was not designed to rely solely on periodic reinvestigations to ensure that cleared people were and remained trustworthy. Everyone involved with handling classified material was charged with looking for and reporting any possible security concerns. With reference particularly to personnel security, the regulations

specified that, if a sailor knew or suspected that someone was committing espionage, he was required to report the facts to his commanding officer or the Naval Investigative Service (NIS). The problem with this requirement is that the evidence shows that very, very few individuals will ever consider espionage as a possible explanation for a co-worker's behavior. John Walker worked closely with hundreds or even thousands of sailors over a twenty year spying career. Many, even most, of those sailors had first-hand knowledge of his unethical behavior and suspiciously large financial expenditures. In fact, John Walker was actively probing a number of them to see if they were good candidates for recruitment into his spy ring. Yet not one of them ever considered that he might be spying.[28]

The issue is even cloudier when one considers issues that are of security interest, but are not in and of themselves crimes--such as heavy alcohol use, personal crisis, or financial difficulty. As seen in the section above on granting Top Secret clearances, reliable information about the security implications of specific behavior or character traits was not available even to the professional, full-time investigators and adjudicators in the DIS. The sailors who should have been looking for and reporting on security risks did not even have the benefit of vague instructions to think about security and use common sense to guide them that DIS agents had. There was no standardized program, or even clear guidance, on reporting misbehavior or possible security risks. Sailors had little reason to think that their observations were security-relevant or grounds for taking action, nor did they have any clear picture of what options for action were feasible or appropriate.[29]

Reporting possible security issues also went against a powerful cultural component of American society in general and the military in particular. As the PERSEREC study of espionage cases puts it:

> Executive Order 12968, *Access to Classified Information*, states that "Employees are encouraged and expected to report any information that raises doubts as to whether an employee's continued eligibility for access to classified information is clearly consistent with national security." This expectation cuts across the strong disinclination in American culture to "rat" on a peer, as well as across the determination to mind one's own business as the best way to get along with co-workers.[30]

This tendency was much more pronounced in the military, because the only means to report such security concerns was the command channel. That meant in practice that sailors were highly reluctant to voice any unease that they had over the disarray in a colleague's personal life, because such a comment could very easily result in criminal or administrative prosecution, demotion, or disciplinary discharge from the Navy. Is it any surprise that the average sailor, who had no reason to know what the security implications of his colleague's unsavory lifestyle were, would keep quiet rather than make a complaint and start a process that may have ruinous results for a shipmate? Furthermore, there are clear negative consequences for a sailor being labeled an "informant," particularly if he is living and working on a ship with the same small group of sailors who saw him causing problems--or indeed, living and working in close proximity with the subject of the complaint himself.[31] Far better to simply keep quiet. As Arthur Walker later said, "a lot of people just tend to mind their own business."[32]

Not only are sailors reluctant to report possible problems to their commanders; their commanders are often unenthusiastic about receiving such reports and forwarding derogatory information up the chain of command. In addition to the same forces listed

above, commanders and supervisors faced additional pressures. First, they were worried about reducing morale in their units. More than anything else, military leaders are charged with developing cohesive, highly motivated units. After all, any sailor might be called on to give his life trying to save his ship or his shipmates--possibly without warning, on immediate instinct; possibly with enough time to be fully aware of what is being asked of him. It is impossible to achieve this level of motivation and self-sacrifice if the sailors believe that co-workers are "spying" on each other and passing on innuendo and rumor behind their backs. Likewise, it is impossible to achieve if sailors believe that any sign of weakness or disarray in their personal affairs will result in loss of their security clearance, job, rank or pay.

Supervisors and commanders also know that they are rated by their superiors in large measure on how their unit appears from the outside--in efficiency, discipline, and morale. This gives them a powerful incentive to keep messy personal problems quiet. This does not mean that Navy supervisors were behaving in an unethical way by covering up known security predicament. Rather, it means that commanders and supervisors had never been given any reason to be aware of the security implications of some of their subordinates' behavior. There was no guidance on what should be reported, or to whom. There was not even any central clearinghouse for security information that they could reference. What little written policy existed was vague to the point of incoherence. A good example is found in the Stilwell report:

> It is improper to impose suspension or termination of a security clearance as a penalty for security violations. Nevertheless, adjudicative authorities should be permitted to suspend a security clearance in cases where an individual has clearly demonstrated an unwillingness or inability to protect classified information, pending readjudication of the clearance.[33]

So what should a supervisor do? It appears that the committee is saying that it is "improper" to suspend a person's clearance for security violations, but that it nevertheless should be done, at least until the adjudicator's decision is overridden by someone else. And remember, this guidance was written *after* 1985, the "Year of the Spy," and is the committee's attempt to clarify and tighten the personnel security system.[34] Nor is it apparent what is expected of supervisors in cases where a subordinate has not "clearly demonstrated an unwillingness or inability to protect classified information," but is instead going through a personal crisis (like financial difficulty) or demonstrates unsavory or unethical behavior that is not work-related (like heavy gambling or marital infidelity). John Walker's supervisors apparently never thought that he showed an unwillingness or inability to safeguard classified information, even though they believed him to be morally compromised. Typical is Bill Metcalf, John Walker's supervisor in the submarine fleet message center at Norfolk during 1968:

> The problems with Johnny Walker involved moral turpitude. The guy just didn't have any moral standards as far as I was concerned. He constantly bragged about women and if a woman looked twice at him, why he'd be unzipping his britches. But there was never any hint that he was mishandling cryptographic material.[35]

It is not clear, even in retrospect, that John Walker's supervisors had sufficient grounds to remove his security clearance under the policy and guidance they had been given.

The personnel security system explicitly depended on supervisors spotting individuals with problematic behavior and removing them from access to sensitive information. Indeed, supervisors were seen as the people *most likely* to identify security risks and were considered *more* reliable at weeding out bad security risks than DIS investigations or records checks.[36] Yet there is virtually no evidence that anyone told the supervisors themselves of this key role; certainly, they were never given even the

absolute minimum level of information (what to report, and to whom) that they would need to carry out their duties effectively.

One final factor contributed to the weakness of the personnel security system: some commanders compounded the problem with a casual or disdainful attitude toward security matters as well.[37] Their approaches toward compliance with security regulations had an enormous impact on the outlook and actions of their subordinates. This was particularly true in the Navy, because both by law and by tradition, ship captains have near absolute authority over everyone and everything that happens aboard their ships. As mentioned previously, the Navy gave commanding officers the authority to allow or deny any of their sailors access to any information, equipment, or spaces onboard the ship. A commander who treated security restrictions as irritating nuisances or as optional recommendations set a powerful precedent for violating regulations. Indeed, he could easily place his subordinates in a position where they felt *forced* to violate security policy. Given that, for a system like FBS that depends on cryptographic keys for its security, a security compromise *anywhere* meant a security compromise *everywhere*, this was almost guaranteed to cause a systemwide failure.

The whole problem of co-worker and supervisor responsibility to report and act on potential security violations can be summed up in two words: divided responsibility. No one seemed to have overall responsibility for identifying and acting on security risks. The administrators who wrote the personnel security policy and the professional investigators in DIS assumed that the cleared person's supervisor and co-workers were best positioned (and hence primarily responsible for) detecting security-relevant facts. It is not an unreasonable assumption--after all, they have much more extensive contact with

the subject than an outside investigator could possibly have, and they should know if and when the subject's personal situation changed for the worse. The extremely low rejection rates for security clearances seems to indicate that the DIS investigators were assuming that anyone submitted for a clearance had already been thoroughly vetted by his supervisor and found to be trustworthy, and their job was to report by exception.[38] Yet no one provided supervisors with even the minimum level of information to carry out their duties. It appears that, in light of this total absence of clear policy and institutional support, most supervisors assumed that the primary responsibility for evaluating security risks remained with the professional investigators. If the professionals, who (presumably) had access to additional information, detailed criteria for decision making, and thorough knowledge of the applicable policies and protocols, thought that a given person was trustworthy, then surely they must be. And so the personnel security system, as implemented, was left with a gaping hole in it. Very little derogatory information was ever brought forward for action, even in cases where there was a very clear pattern of security issues with a given individual.[39]

Investigating Espionage

The final part of the personnel security system was the professional investigation of possible espionage by law enforcement agencies. Yet even here, the system was far more complex and ad hoc than necessary. To start with, questions of which organization was responsible for the investigation were far from clear. By law, the FBI is the lead agency for tracking suspected foreign intelligence agents in the US. Counterintelligence investigations were done by the FBI within U.S. territory, and as a joint FBI/CIA task force if overseas. At least some overseas involvement occurs in many counterintelligence

investigations; for example, in the John Walker case, all but two of his meetings with his KGB handlers occurred overseas, in places such as Vienna, Hong Kong, and Morocco.[40] Additionally, the Army Intelligence and Security Command, Naval Investigative Service (NIS), and Air Force Office of Special Investigations were tasked to investigate crimes by members of their service departments; but this was in addition to, not instead of, the FBI and CIA responsibilities in the case. Thus, once the John Walker case finally broke in 1985, the case was being worked simultaneously by the FBI and NIS, with some involvement by the CIA as well.[41]

SA Robert Hunter, the FBI special agent who arrested John Walker had this to say about the Navy's in-house investigators: "During my 23 years of contact with the Naval Investigative Service, I reached the conclusion that it was one screwed-up outfit."[42] He identified four reasons for its poor performance. First, NIS investigators were very poorly trained. Indeed, in some cases they sent out to the field completely untrained![43] Second, the investigators were civilian employees who were working directly for line officers in the Navy, who had no investigative experience at all. This led to a number of serious problems with prioritization and investigative guidelines. Investigators had little authority or latitude in working cases. SA Hunter further believed that most Navy officers were more concerned about protecting their careers than seeing criminals prosecuted, and so they would meddle in investigations to prevent bad news from surfacing.[44]

Navy officers were not the only ones who had reason to want to bury espionage investigations. There is an inherent conflict of interest within the government regarding the prosecution of espionage cases. Most importantly, putting a suspected spy on trial requires the government to reveal precise details of the classified material that the

accused handed over and details of how he had been identified as a spy. Since in most cases this involved highly sensitive "sources and methods" information--that is, the identities of US intelligence agents and foreigners spying for the US or details of the government's ability to intercept and decrypt foreign governments' communications--there was a genuine concern that prosecuting spies would cause more harm than good. From the mid-1950s to the mid-1970s, the US government was extremely reluctant to prosecute accused spies in open court, even when evidence of their guilt was overwhelming. Indeed, during the period under study in this report (1967-1974), fewer than eleven individuals were prosecuted for espionage or attempted espionage.[45] As the PERSEREC report on espionage by US citizens puts it:

> The Justice Department during these years [1947-1977] agreed with the position of the intelligence agencies: that prosecuting spies did more harm than good because it was likely to invite retaliation against Americans abroad; it ruined intelligence agents as assets for future use; and it revealed to our adversaries what we did and did not know. The preferred approach was to identify and quietly neutralize spies in order to control the loss of secrets and to avoid the admission of failure that a spy represents.[46]

Dr. Herbig and Dr. Wiskoff also note that counterintelligence efforts were further impaired by political meddling from the Johnson and Nixon administrations: the FBI was directed to divert counterintelligence resources to surveillance and disruption of American antiwar and civil rights groups. The CIA also diverted resources into investigating possible foreign influences on American groups opposing US government policies, leaving less available for overseas counterintelligence missions.[47] Ironically, had John Walker been exposed in 1974, or been discovered based on classified intercepts, he may very well have escaped punishment for his crimes.

A major change in US counterespionage policy occurred in the mid-1970s. The political decision was made to begin prosecuting spies, even at the risk of compromising US sources and methods. Congress passed two laws that became the key to counterintelligence investigations: the Foreign Intelligence Surveillance Act (FISA) in 1978, which established panels of specially cleared District judges to issue wiretap warrants for counterintelligence investigations, and the Classified Information Protection Act (CIPA) in 1980, which set rules for the handling classified materials during court proceedings. In particular, CIPA allowed the trial judge to hold private evidentiary hearings to rule on whether defense attorneys could compel the revelation of classified materials, and it allowed the judge to enter unclassified summaries of classified documents into evidence. These provisions removed the risk of a defendant making threatening to reveal classified information if the government pushed for conviction on serious charges (so-called "greymail"). FISA and CIPA have been critical in all subsequent prosecutions of accused spies in the United States. The evidence against John Walker and his confederates was collected using FISA warrants, and the subsequent trials were conducted under CIPA rules, which made convictions much easier to obtain.[48]

The key point to remember about this is that FISA and CIPA were not available to prosecutors when the version of FBS under study in this report was being designed and implemented. The official position at the time was that individuals who were behaving suspiciously would be turned over to professional investigators at the NIS or FBI. Those investigators would uncover the facts and prosecute the guilty; furthermore, persons who were considering espionage would be deterred by the chance of being caught and prosecuted. Yet this whole chain of events was demonstrably flawed. Extremely few

"suspicious" cases were turned over to law enforcement investigators. The agencies charged with investigating were underresourced, misdirected, and suffering from extensive personally or politically motivated meddling. Investigators had no means of getting legal wiretap orders without revealing classified material; resorting to illegal wiretaps meant that the evidence gained would be inadmissible in court, among other problems. Even when the evidence was legally acquired and totally clear, the US government policy was so strongly against prosecution that virtually no spies were convicted. The personnel in charge of designing and implementing FBS should have known that counterintelligence investigations and prosecution under the federal espionage laws were almost entirely empty threats.

John Walker's reaction to his arrest by the FBI is a good illustration of how spies viewed the risks of a counterintelligence investigation. He was arrested in a motel, while in possession of detailed information about how and where to leave a large bag of classified information for his Soviet handler to get it, and where to pick up his payment of money. He knew that the FBI had caught him with enough information to prove he had been spying. Yet he spent his first day under arrest confidently awaiting the arrival of Justice Department lawyers, who would present him with a deal--immunity from prosecution, if he would explain what he had compromised and how he had pulled off his daring feat; or perhaps work as a double agent, passing bogus information to the Soviets and being paid by both sides. When it slowly dawned on him that no deal was coming, he was outraged. It was only the minor, amateur spies that got treated as common criminals; he was a major, important spy, and he had never seen big-league spies treated as he was

being treated. The decades of poor-quality counterintelligence work and failure to prosecute spies had eliminated any thoughts of deterrence from his mind.[49]

Summary

In summary, the personnel security system appeared to be a solid, workable solution to the need to keep classified information out of untrustworthy hands. However, on closer inspection, the system was far less comprehensive than it seemed. The process for investigating personnel for Secret-level clearances was extremely cursory--it was incapable of uncovering the great majority of criminal convictions, and it made no effort whatsoever to check any other security-relevant areas, such as finances. Even such a minimal vetting process was routinely undermined by people with vested interests in concealing information. Granting Top Secret clearances involved a more elaborate series of checks; however, the results were still highly untrustworthy. DIS and the adjudication system were chronically underfunded and undermanned, there was virtually no reliable scientific information on which to base decisions, and the Navy allowed commanding officer to override the adjudicators' decisions anyway. Periodic reinvestigations were almost always backlogged by several years and could, in any event, be easily avoided by tampering with personnel records. Policy existed that required supervisors and co-workers to report suspicious behavior to the authorities, yet almost no one did; however, the policy makers apparently made no effort to find out whether their policies were being followed, or even if sailors knew the policy existed. Even if sailors had reported suspicious behavior, the law enforcement agencies charged with investigating and prosecuting espionage were divided, distracted by political meddling, and had few good legal methods available to them for collecting and presenting evidence in court. The

official government policy towards espionage made covering up the crime more important than punishing criminals; the result was a climate of minimal deterrence for potential spies. All of these facts should have been known to decision makers who were designing FBS in the mid-1960s, if they had looked into the matter; yet no one did look into it in a systematic way until the Stilwell commission in 1986.

---

[1]Early, 108.

[2]Richard G. Stilwell, General, USA, Ret. (Chairman), *Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Policy and Practices*, November 19, 1985; available from http://www.fas.org/sgp/library/stilwell.html, Executive Summary and Requests for Initial Clearances; Internet.

[3]Ibid., Organizational Arrangements.

[4]Ibid., Organizational Arrangements.

[5]Ibid., Initial Investigations.

[6]Early, 30-31.

[7]Ibid., 31.

[8]Ibid., 32-33.

[9]Ibid., 33.

[10]Stilwell, Initial Investigations.

[11]Ibid., Initial Investigations.

[12]Early, 50-51.

[13]Hunter, 26.

[14]Early, 51.

[15]Ibid., 52.

[16]Ibid., 45 and 50-55.

[17]Stilwell, Adjudication.

[18]Ibid., Adjudication.

[19]James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Boston: Houghton Mifflin, 1982), 82.

[20]Early, 51-52.

[21]American Psychiatric Association, "Position Statement on Homosexuality and Civil Rights," *American Journal of Psychiatry, 131 (4),* (15 December 1973), 497.

[22]United States General Accounting Office, *Security Clearances: Consideration of Sexual Orientation in the Clearance Process.* Report to Congressional Requesters, GAO/NSIAD-95-21, 24 March 1995, 1-3 and 9-10.

[23]Stilwell, Periodic Reinvestigations; and Katherine L. Herbig and Martin F. Wiskoff, Defense Personnel Security Research Center, *Espionage Against the United States by American Citizens 1947-2001*, PERSEREC Technical Report 02-5, July 2002, xiii.

[24]He said that he did provide the information requested; however, a thorough counterintelligence investigation after John Walker's confession failed to turn up any evidence of espionage by his co-workers in the NAVCAMS. See Early, 68.

[25]Ibid., 56.

[26]Ibid., 68-103.

[27]Ibid., 109.

[28]After John Walker had been captured by the FBI, the NIS attempted to interview every sailor that had ever either worked with him or had had any social contact with him--even those who had only gone to the same cocktail party as him. Many of these interviewees were polygraph tested as well. It was wholly wasted effort; there was no evidence that any of them had ever considered espionage as an explanation for his behavior. See Hunter, 155-159. It is worth noting that some spies have been apprehended based on co-workers' reports. Herbig and Wiskoff specifically highlight the cases of Jonathan Pollard, Michael Allen, and Samuel Morison as resulting from co-worker tip-offs to investigators. However, these cases are a tiny minority of the 150 documented cases of espionage they compiled in the PERSEREC database. They present a number of counterexamples, including the case of Jeffrey Carney, where he himself asked his supervisors cancel his security clearance and relieve him of his duties due to his psychiatric problems. They refused, citing a shortage of replacements with Top Secret/SCI security clearances. Sgt. Carney began spying for the East Germans shortly afterward. See Herbig, 56-59.

[29]Stilwell, Continuing Command/Supervisory Evaluations.

[30]Herbig, 59.

[31]Stilwell, Acquiring Information from Additional Sources.

[32]Herbig, 59.

[33]Stilwell, Taking Effective Action Against Those Who Violate the Rules.

[34]A total of 35 US citizens were active in, and eventually convicted of, espionage or attempted espionage during 1985. This includes the four members of the Walker spy ring. See Herbig, 61.

[35]Early, 81-82.

[36]Stilwell, Continuing Command/Supervisory Evaluations and Commander/Supervisor Emphasis.

[37]Ibid., Commander/Supervisor Emphasis.

[38]The Stilwell commission found that rejection rates were between 2.5 percent and 0.2 percent, depending on the group of applicants considered. It is worth noting that this is for initial investigations. It was perhaps unwise for DIS to assume that an applicant's supervisor had vetted him at all, since most of them probably could not start working for the organization that submitted them until after receiving the approval. See Stilwell, Adjudication.

[39]Ibid., Continuing Command/Supervisory Evaluations.

[40]Early, 65.

[41]Hunter, 154.

[42]Ibid., 154.

[43]Ibid., 154.

[44]Ibid., 154.

[45]Nine military members were prosecuted for espionage in the period 1966-1975, as compared to only two civilian government employees. The number of persons suspected of espionage during that period has never been published in an unclassified document; it would appear that most suspects were either eased out of their jobs or pressured to become double agents, giving their handlers bogus information. The clearest examples of known spies escaping prosecution come from the Venona intercepts. These were Soviet diplomatic cables transmitted in the 1940s and 1950s; the NSA was able to decrypt some of these messages and has subsequently declassified and published them during the 1990s. The material includes reports from KGB agents operating under

diplomatic cover at the UN mission and at the Soviet embassy in Washington, DC, and identified a number of US citizens by name as spies. The intelligence community convinced the Justice Department that revealing the Venona intercepts in court would reveal the NSA's ability to decrypt their cables and cause a catastrophic loss of critical intelligence. Accordingly, a number of the named individuals were able to stonewall the FBI and escape prosecution entirely. For example, Theodore Hall was a physicist who passed the Soviets information on the US atomic bomb program in 1943; although both his identity and the secrets he passed were known from the intercepts, he was never prosecuted and lived out the rest of his life in Cambridge, England. See Herbig, 7-10.

[46]Ibid., 8.

[47]Ibid., 8.

[48]Ibid., 8-12; Hunter, 71-92.

[49]Earley, 11-14.

CHAPTER 3

TECHNICAL SECURITY

> The KWR-37 has stopped breaking. With other systems [including the KW-7], there is no problem. But KWR-37 won't break anymore.[1]
>
> John Walker's KGB handler, at a meeting on 30 June 1979, quoted in *Breaking the Ring*

Overview of Technical Security

Technical security is a general term for the security features designed into COMSEC devices that make recovering classified data from the transmitted message impossible for anyone except the legitimate recipient. Another way of saying this is that it is the cryptographic equipment's ability to withstand cryptanalytic attack without compromise. This sort of attack is commonly called "code breaking," and it is trying to decipher an encrypted message without knowledge of the key, and possibly without any knowledge of the encryption algorithm either. (The issue of controlling access to the keys will be addressed in the next chapter.) In the most general terms, cryptanalysis involves two steps. First, the adversary must intercept a copy of the encrypted message. As stated in the introduction, FBS was a long-distance, wide-area broadcast, and so interception was very easy; it was assumed that the Soviets (and indeed, anyone else who cared to listen) would get a copy of every encrypted message. The adversary's next step is to apply mathematical formulas to attempt to extract some information out of the encrypted message. This report will not go into the mathematical details of this process. A few general comments will suffice: first, cryptanalysis is usually an iterative process. That is, the analyst makes some assumptions about the cryptographic system and message,

calculates some trial-and-error results, and then refines his assumptions based on the statistical results of his trials. The more the analyst knows about the system and the message, the easier and faster it will be to break the code. Second, the mathematical methods used can hinge on some extremely subtle clues. Some good examples of this can be found in the published reports on the breaking of the German Enigma machines in World War II. For example, the British code breakers took advantage of a German procedural rule that the machine's settings could not be repeated; that meant that, once one day's settings had been determined, the code breakers could positively rule out that particular setting for the next 28 days' worth of traffic--and since there were only 60 possible settings, the steady accumulation of knowledge about multiple days' worth of messages could potentially cut the analytic workload by almost half. They even made effective use of small quirks, like the fact that so many German messages began with the phrase "Heil Hitler," to further narrow their searches.[2]

Being able to break an encryption system without access to the key is the ultimate prize for a national intelligence service, since it allows total access to an adversary's information, essentially without risk. In such a case, there would not be any further need for a spy to steal keys. Indeed, a good measure of its value is the resources which countries will devote to causing such a failure in their adversaries' systems. The U.S. government budget for such activities was (and still is) classified, but during the time period under study (1967-1974), estimates for U.S. government expenditures have ranged as high as $10 billion--in other words, more than the budget for the rest of the intelligence community, combined.[3]

The National Security Agency

The U.S. government has centralized both the protection of its own information and the exploitation of other countries' communications into one agency: the National Security Agency (NSA), formally a part of the Department of Defense but in practice almost entirely autonomous. It was given sole responsibility for both the exploitation of foreign signals intelligence (SIGINT) and for the protection of U.S. government communications (COMSEC); that is, it both tried to break other countries' codes and produce U.S. government codes. It handles some of the most sensitive information that the United States has, and so was (and remains) one of the most secretive government agencies--to the extent that it officially denied its own existence for many years. Under Public Law 86-36, passed in 1959, gives the NSA virtually blanket authority to maintain secrecy: "Nothing in this Act or any other law… shall be construed to require the disclosure of the organization or any function of the National Security Agency, or of any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such Agency." A running joke in the U.S. government held that "NSA" actually stood for either "No Such Agency" or "Never Say Anything."[4] Almost everything that the NSA did was considered Top Secret compartmented information, never shared with anyone outside of the agency itself. The agency also had a well-deserved reputation for technical competence and excellent engineering skills--primarily based on its proven ability to obtain highly valuable intelligence by exploiting a wide variety of foreign communications systems.

During the time period under study (1967-1975), the NSA was organized into a number of suborganizations. The one of primary interest here was the Office of

Communications Security, also called S Organization. It was responsible for the design, testing, procurement, certification and life cycle management of all encryption systems used by the U.S. government. It provided the technical expertise for principles and policy recommendations, which determined the details of how a particular device could be used, who could have access to it, what could be transmitted using it, and so on. S Organization also ran a large production facility and print shop, producing most of the key materials and printed matter pertaining to COMSEC devices. In a sense, the S Organization was the sole point of contact between "customers" (in this case, the U.S. Navy) and NSA; it was the source of all COMSEC equipment, manuals, policy, and key that the Navy used.[5] S Organization was supported with NSA by several other organizations, which did more theoretical research in mathematics, physics, and related fields; the most noteworthy of these was the Standard Technical Engineering Division (STED), later renamed the Cryptographic Equipment Division, which was responsible for research and development of cutting-edge technologies which might eventually prove useful in cryptographic devices.[6]

Officially, all COMSEC policy for the U.S. government was set by the United States Communications Security Committee, which was a cabinet-level committee within the National Security Council. A procedure was in place whereby, in the event of disagreement at the committee level, the proposed decision would be given to the Secretaries of Defense and State for resolution; if they were unable to resolve the dispute, the question would be decided by the President directly. Policy decisions would then be handed to the Department of Defense, as executive agent; the DoD then tasked the NSA, its subordinate, to implement the policy. In actual practice, the decision flow was exactly

the reverse. The USCOMSEC Committee only met once a year and served primarily to rubber stamp decisions made by technical subcommittees; these, in turn, were wholly dominated by the NSA employees, who alone had the detailed technical knowledge necessary, and who were often unwilling to share information with anyone else. Indeed, in at least one instance, the NSA refused to even inform the committee members about what a particular issue was, on the grounds that it was too sensitive for the full committee (that is, the President's Cabinet) to know.[7]

Designing Cryptographic Systems

As mentioned above, the NSA is solely responsible for designing cryptographic systems. The design process for a cryptographic device begins when a user designs a new communication system (in this case, the U.S. Navy designing FBS). Cryptographic engineers from NSA first had to evaluate the proposed communication system to determine what potential security weaknesses it might have. Encryptors cannot simply be added to a radio or teletypewriter, because very minor and subtle details might give an adversary highly valuable clues useful in breaking an encryption system. This analysis phase could take several years. Once that stage was complete, the NSA engineers determined if an existing encryption device could be used (or modified for use) in the communications system, or if a totally new device was needed.[8]

That decision was influenced by a number of factors, and the decision to develop the KW-7 is a good example of the process. Before the fielding of the KW-7, teletypewriters had been secured with encryptors such as the KL-7 and KL-47, which used a series of spinning rotors to shuffle the characters in the output. This is the same method used by the Japanese "Purple" and German Enigma machines in World War II.[9]

One problem with rotor-based systems is that there are limits to how fast the rotors can spin; the Navy's new, faster teletypewriters were pushing (or exceeded) the physical restrictions of such encryptors. This was an excellent reason to justify why a totally new device needed to be developed--a development effort that would take years, potentially cost hundreds of millions of dollars, and had a real risk that the end product would be unsuitable for its true operating environment once it was fielded to the fleet.[10]

There was a much more persuasive argument for designing a new family of encryptors, fully known to the NSA at the time but apparently never discussed with anyone outside the Agency. The NSA (and its predecessor organizations) had been breaking rotor-based systems since the 1930s, most notably the Japanese "Purple" codes and the German Enigma. As these successes demonstrated, rotor-based encryptors were unquestionably vulnerable to cryptanalytic attack if the adversary had sufficient computing power available. The KL-47 was more complex than the Enigma, but the power of computers was increasing exponentially fast since World War II as well. It was clear that it was only a matter of time before the complexity of computers caught up with the encryptor. But remember: the story of the breaking of the Enigma machine was not revealed in public until 1979, and then by a British code breaker; during the time period under study, the information was still Top Secret compartmented data. There is no record that the NSA ever told anyone outside of its own organization that rotor-based encryptors similar to the KL-47 had been broken in the past and were growing increasingly vulnerable to attacks using modern computers. Indeed, the KL-47 remained certified for use with Top Secret data and was still in active use in some locations as late as the mid-1970s.[11]

The importance of this fact is that the U.S. Navy, which was responsible for the data to be protected by these cryptographic devices, was deliberately left in ignorance about the true risks of using the devices. The NSA only issued a certification packet stating that a particular device, used in a particular way, was approved for use with data up to a particular security classification. The implication was that the NSA's own code breakers had attempted to penetrate the system and failed; and since the NSA code breakers were the best in the world, then naturally every other country's code breakers would also fail. Privately within the NSA, there were some concerns that this might not really be true. Lt. Gen. Marshall Carter, a former director of NSA, had this to say in 1982:

> We operated on the alleged mystique that anything COMSEC did was ground through the operational side of the cryptologic branch to see if they could get into it. . . . That was what we were supposed to do; that was what we said we were doing . . . [but] I wasn't technically oriented enough to know whether in fact we did do it.[12]

The problem is more difficult than simply wondering whether the NSA followed up on its commitments to test thoroughly. Any security evaluation will involve assumptions--some about what the adversary is capable of and what resources he will devote to this particular target, some about what the operators will do, some about the equipment and environment, and so on. There is no evidence that these assumptions were ever checked for validity in any systematic way, or even stated to the end user. For example, there is no evidence that the NSA ever asked the U.S. Navy any questions about how likely it would be for the sailors operating the encryptor to cut corners when implementing particular policy proposals. It is obvious that the more burdensome the policy on the operator, the more likely that it will be bypassed in practice, and equally obvious that the U.S. Navy

officers and petty officers are best placed to know what their sailors are probably going to do in an operational environment. Yet there is no evidence that the NSA asked Navy leaders questions about possible compliance rates for given policy restrictions. It would appear that 100 percent compliance was assumed, irregardless of how burdensome the requirements placed on the operators were.

The case of the KL-7 and KL-47 shows another problem with assumptions. The device was certified in the early 1950s, based in part on some assumptions about the technological capabilities of the Soviet Union. At that time, the USSR had essentially no computer capability at all and little perceived code breaking ability; consequently, the KL-7 and KL-47 were considered secure against any reasonable attack that the USSR might mount against them, and they were certified for Top Secret data. While those assumptions *might* have been true in 1950, they were obviously false by 1970. In other words, even if all of the initial assumptions are true, they can become false over time. The NSA may have done some internal re-evaluations of the vulnerability of the KL-7 and KL-47 in light of the major improvements in computing capability available, but there is no evidence that any such re-evaluation was briefed to the organizations actually using the devices to protect their data. All indications are that the Navy (and other organizations) were simply told that the NSA had tested the device, and it was certified for use with classified data.

The Soviet Approach to Breaking the KW-7

Clearly, the Soviets were extremely interested in causing a technical security failure of the KW-7. They knew that they could not ensure that John Walker (or another spy) would always be placed to give them the keys in a timely manner; if they could

decrypt the messages without the key, they would have permanent, uninterrupted access to every broadcast. This raises the question: what things would they need to have to mount a systematic attack on the encryptor? They boil down to two major items: as much data as possible on the device's internal workings--ideally, one or more working copies of the encryptor, plus the complete operation and repair manuals--and detailed specifics on any changes that might be made to the device from time to time.

One of the very few things John Walker did *not* give the Soviets was a working copy of an encryptor. Unfortunately, they did not need him to do so, as the U.S. Navy was about to all-but-deliver functional KW-7s to the Soviets, in the shape of the USS *Pueblo* (AGER-2). She was a minimally armed, barely seaworthy cargo ship that had been modified to perform electronic intercept missions off the coast of North Korea. On 23 January 1968, she was attacked by North Korean gunboats and aircraft and was captured. She had been carrying very large amounts of classified material, plus a number of encryption and intercept devices, and despite valiant attempts, the crew was able to destroy less than 10 percent of the material. According to Oleg Kalugin, a former KGB major general, the North Koreans captured and passed on to the Soviet Union working copies of the KW-7, as well as a complete set of operation and repair manuals.[13]

Nonetheless, a close analysis of the details shows that John Walker probably did have a role in causing the USS *Pueblo* incident. From the Soviet standpoint, instigating the capture of a U.S. Navy ship, even second hand, would be a highly risky move, and would only be done if they thought that there was a correspondingly large payoff. Capturing one or more working copies of encryptors might fit the bill; but there is one problem: they could reasonably expect that the U.S. would respond to such an obvious

compromise by making some changes to the encryptor, which would render the seized copies unusable. The U.S. did, in fact, do so; and the Soviets had John Walker giving them copies of the change orders that allowed them to modify the seized devices when the changes were made.[14]

Since the USS *Pueblo* incident happened so soon after John Walker began spying, and since John Walker was placed to give the Soviets exactly what they needed to make the best use of the items seized from the ship, it naturally raises the question of whether the two events were related. While the conclusion is not iron-clad, the balance of the evidence indicates that they were: that the Soviets asked the North Koreans to capture the USS *Pueblo*, because they knew that they would have the information they needed to exploit the seized equipment to the maximum extent.

There are two sources of evidence for this: John Walker himself, and Oleg Kalugin, the KGB general. Kalugin claims to have been John Walker's first handler, and to have knowledge about a shipment of some 792 pounds of equipment and documents seized from the USS *Pueblo* and sent from North Korea to the USSR.[15] He gave an interview to Special Agent Robert Hunter, the lead FBI agent on the Walker case, and said that he thought that the USS *Pueblo* seizure happened too soon after John Walker began spying for the Soviets to have used the information he gave them to influence the seizure--although he admitted that the Soviets "definitely" would have asked the North Koreans to seize the ship if they could have known where it was, or what it had on board.[16]

That would seem to exonerate John Walker from responsibility for the USS *Pueblo* seizure. Yet Mr. Kalugin is probably not being totally honest in his descriptions

of events. He is not a defector. After clashing with his superiors in 1990, he was fired from the KGB and stripped of his pension. He won a seat in the Russian parliament on a reform platform, but only served one term. After that, he published a book and has made his living giving speeches, interviews and lectures about his time as a KGB agent, but he is not formally cooperating with Western intelligence agencies. This is important, because in his book he makes it clear that he retains some loyalty to the spies he worked with. A close reading of his book bears this out. Spies who have never been publicly identified are described in an extremely vague way, such as "an ambassador from a large Arab country… [who] passed me cables and other documents"[17]--never enough details to identify the person, or the precise information they revealed. In the cases of those spies who *have* been identified previously, he sticks very close to the published accounts of their doings. In John Walker's case, he strictly follows the details laid out in the book *Family of Spies* by Pete Early, which is based on jailhouse interviews Mr. Early conducted with John Walker while he was awaiting sentencing.[18] That is very interesting, because it is now clear that some of those details are definitely false.

John Walker's original story about how he began spying was that it was an impulsive action, taken in a moment of extreme financial and family stress in December, 1967. He gave a very detailed description of how he copied whatever classified documents he had easily available while on the night shift, and how he walked into the Soviet embassy to volunteer to spy. Those details tripped him up. His description both the inside and outside of the Soviet embassy in Washington, DC was absolutely accurate--except that he described it as it appeared after a new security fence was installed in 1974, rather than how it appeared in late 1967.[19]

Furthermore, the FBI gave him extensive polygraph tests[20] as part of his counterintelligence debriefing, and John Walker repeatedly failed polygraphs on the original, "overwhelming impulse" version of how he started to spy. He did, however, pass a polygraph on the following statement:

> I know you believe I'm lying about the beginning of the operation because of [my failing] the polygraph and the fence story. Let me give you a scenario: [my brother] Arthur got in some type of financial trouble, probably in New York, and became involved with a number of New York loan sharks. Art needed money desperately, and I gave him some classified documents to sell. After Art sold the documents and got some money, he became frightened and wanted to drop out. I saw no harm in selling the information to the Soviets, as the countries were not at war and would never go to war. I felt it was an easy chance to make some money, so I walked into a Soviet embassy somewhere in the world.[21]

Thus a more likely story is this: John Walker had first stolen some classified information for his brother, probably sometime around 1965-66. He was pleasantly surprised to find out how easy it was and how much money could be made doing it; and when his brother got cold feet, he decided that he would continue on his own. He pilfered or copied some documents while at sea onboard the USS *Simon Bolivar* (SSBN-641),[22] and at a port call "somewhere in the world," he walked into a Soviet embassy, gave them the documents as proof of his bona fides, and offered to spy for them. He told them that he was going to be assigned as a watch officer at NAVCAMS Atlantic fleet, and he would have high-level access to cryptographic materials there for a number of years. The Soviets were extremely pleased, paid him enough money on the spot to whet his appetite for more, and gave him a "shopping list" and instructions on how to do his first dead drop in the Washington, DC area--with the time set for mid-December, 1967, a few weeks after he signed in at Norfolk. Barbara Walker was certain that John Walker first showed

up with a lot of unexplained money just before Christmas, 1967, so by then he was definitely making deliveries of classified material to the Soviets.

The timing is important for determining if the USS *Pueblo* seizure was related to John Walker's decision to start spying. If the Soviets knew several months in advance that they would have an agent who could get them the KW-7 keys and any manuals or change orders that might come out, then the value of seizing a functional KW-7 increased dramatically. Kalugin made some vague and rather coy comments that the Soviet Union "definitely" would have asked the North Koreans to seize the ship if they had enough advance knowledge… and it seems extremely likely that they did, in fact, have considerable advance knowledge that John Walker was going to start delivering high-quality COMSEC material in December 1967. Thus, the balance of probabilities is that the Soviets instigated the USS *Pueblo* seizure as a means to further exploit the material that John Walker began providing in late 1967.

Was the KW-7 Broken?

Thus, it is clear that the Soviet attempts to break the KW-7 seem to have had three steps: recruiting John Walker to provide them key material and manuals, seizing a physical copy of the KW-7 from the USS *Pueblo*, and extensively analyzing the machines and manuals they had to determine a way to break the KW-7 *without* getting a copy of the keys. But did they succeed? Were they able to decrypt material encrypted by the KW-7 *without* getting the keys, due to their knowledge of the inner workings of the device?

That question has never been answered in an unclassified publication. The only people who know for certain are the Soviet intelligence agencies, who were examining

the intercepted messages. They obviously do not publish the details of their sources and methods, so concrete proof is not to be had. The US government presumably conducted a detailed analysis of the possibility of the KW-7 being compromised, based on John Walker's espionage, but no such analysis has been published in the unclassified literature. Thus, we are left with drawing only tentative conclusions, based on circumstantial evidence; however, the evidence that is available hints that the Soviets were successful in breaking the KW-7.

The first major source of information is the unclassified portions of John Walker's debriefings, plus his comments to a handful of reporters prior to his sentencing. The first bit of evidence is that John Walker said that his Soviet handlers changed their emphasis on how important the prompt delivery of key materials was over time. In particular, he reports that, at the beginning of his spying career, his handlers were pushing him strongly to deliver key material to them very regularly. According to SA Hunter, the "average" Soviet spy delivered a package of materials to his handler once or twice a year; in contrast, John Walker was delivering material every two to three months at the beginning.[23] This is important, because spies and their handlers are most vulnerable to capture during the handoff of material--indeed, that is in fact how the FBI caught John Walker. So the Soviets were willing to risk losing such a valuable spy in order to get the material faster, in 1968 and 1969. But John Walker reported that, beginning in 1970, his handlers began pushing him to hand off material less frequently--only once every six months.[24] This means that his handlers were abruptly much less interested in "hot" data. One explanation for this is that, after two years of studying the captured KW-7s and the manuals and the key material that John Walker had been giving them, they were able to

decrypt some or all of the messages without having the key. That alone is not conclusive, however. It may mean simply that the Soviets had recruited another spy and were getting the keys from someone else, for example. Alternately, they could have changed their minds about the risk/benefit balance between the short-term value of "hot" keys versus the long-term benefit of keeping John Walker hidden from the authorities and providing material for many years.

Yet there is still more evidence of compromise of the KW-7 to be found in John Walker's public statements. He said that he had a meeting with his KGB handler in Vienna on 30 June 1979. By this point, John Walker had stopped spying directly and had only recruited one spy, Jerry Whitworth, into his ring. He remembered his handler telling him that they could no longer break the KWR-37. Some internal modification must have been made, and they needed the technical specifications urgently. The KGB agent mentioned in passing that there was no trouble with the other systems, which included the KW-7.[25] Again, this implies that the Soviets were able to decrypt the KW-7 traffic without further assistance from their spies.

More evidence is available from the public statements made by several high-ranking individuals in the Navy in the aftermath of the capture and trial of John Walker. Most important of these are comments by Secretary of the Navy Lehman made to the *Washington Post* in an article published on 13 October, 1986, which implied that the Soviets knew enough to break some systems without having a key.[26] His comments, and similar comments made by other officials both in the press and at the Walker spy ring trials, do not identify the KW-7 specifically. This is important, because John Walker is known to have compromised a number of systems, including older and less-capable

systems such as the KL-47; Secretary Lehman may have been referring to one of these systems rather than the KW-7. Likewise, these comments do not give an estimation of how much information the Soviets would have recovered, or what delays they would have encountered in attempting to decrypt messages without keys. As mentioned previously, if the Soviets had both the key and a working KW-7, they would have been able to decrypt 100 percent of the messages real time--that is, as fast as the US Navy recipients could decrypt them. In historical examples of cases where cryptanalysts do not have the keys to a system directly available, decryptions take far longer and typically result in decryption of only part of the message traffic. For example, in the spring of 1942, American cryptanalysts managed to decrypt an average of 10 to 12 percent of the Japanese Naval messages, with an average delay of two to three weeks.[27] So even if Secretary Lehman's comments are specifically about the KW-7, it may be that only part of the message traffic was available to the Soviets without the keys, and there might have been significant delays in getting that part of the information as well.

In conclusion, one cannot say with absolute certainty, based on the unclassified evidence available, that the Soviets were able to read traffic encrypted with the KW-7 without the traffic keys. However, there is strong circumstantial evidence that they were able to retrieve some, perhaps all, the information from the KW-7 even without getting the daily keys from a spy.

---

[1]John Barron, *Breaking the Ring (*Boston: Houghton-Mifflin, 1987), 186.

[2]Greg Goebel, "British Codebreakers in World War II" (date unavailable), http://www.vectorsite.net/ttcode8.html#m3, "Bletchley Park Against Enigma," downloaded on 5 March 2005.

[3]Bamford, 77.

[4]Ibid., 281.

[5]Ibid., 93.

[6]Ibid., 96-97.

[7]The end result was that the NSA's deputy director for COMSEC personally briefed the Secretary of State and Secretary of Defense. They both approved the policy change that NSA had requested. All other details about this incident have remained highly classified. See Bamford, 94.

[8]Ibid., 95.

[9]The KL-47 was another one of the systems that John Walker compromised. When the FBI searched his house after his arrest, they found a special device that the KGB had given him in 1967, which revealed the complicated internal wiring which performed the shuffling of characters. John Walker also admits to giving the Soviets full copies of the manuals, which would have allowed them to construct a duplicate KL-47 at will, and complete key lists. Since the Soviets were able to give him the device within three weeks of him starting to spy, and since another Soviet spy, Army Sergeant Joseph Helmich, was caught with an identical device in the mid-1970s, we can assume that Walker was definitely not the first person to sell out the KL-47. See Hunter, 85-86.

[10]An example of a failed project was the KY-28, a voice radio encryptor designed during the Vietnam War for use in fighter aircraft. More than $110 million was spent to develop and field KY-28s, and over 2,200 were manufactured and installed. Combat pilots refused to use them, however, because the lag between transmission and receipt of the message was a dangerous distraction in combat. The result was that US air to ground communications remained unencrypted and vulnerable to enemy exploitation throughout the war. See Bamford, 95.

[11]Jerry Proc, "KL-47" (date unavailable), http://www.jproc.ca/crypto/kl47.html and "KL-7," http://www.jproc.ca/crypto/kl7.html (13 January 2005)

[12]Bamford, 95-96.

[13]Virtually everything failed the crew that day. The ship had an incinerator, but it was located on the deck and consequently was exposed to North Korean gunfire. A backup method was to put materials in weighted bags and throw them overboard, but the bags proved to be too heavy to lift; the ship was also in water shallow enough that they would probably have been recovered easily. There were no explosive or incendiary devices on board, nor were there any means to scuttle the ship. Crew members tried lighting documents on fire in waste paper baskets, which left their work spaces full of choking smoke, and smashed at the cryptographic devices with sledgehammers and fire axes--only to find that the machines had been carefully designed to withstand rough treatment without damage; in some cases, the intelligence devices broke the

sledgehammers, rather than the other way around. Some sailors tried ripping documents into fragments by hand. One panicked crewman was seen trying to flush documents down the toilet, which had ceased working when general quarters was called. The total lack of effective destruction methods is all the more startling when one realizes that both the *USS Liberty* (AGTR-5) and the *USS Banner* (AGER-1) had been attacked during previous cruises. See Mitchell B. Lerner, *The Pueblo Incident: A Spy Ship and the Failure of American Foreign Policy (*Lawrence, Kansas: University Press of Kansas), 79-83.

[14]Early, 72.

[15]Lerner, 83.

[16]Hunter, 216.

[17]Oleg Kalugin and Fen Montaigne, *The First Directorate (*New York: St. Martin's Press, 1994), 77.

[18]Ibid., 84-90.

[19]Hunter, 122.

[20]Polygraph tests are sometimes called "lie detector tests," but this is a misnomer. They are not able to detect truth or falsehood. Rather, they measure some unconscious physiological responses to stress (such as sweating, heart rate increases, and breathing changes). Most people find it more stressful to lie than to tell the truth, so a polygraph can indicate the difference between someone attempting to deceive the tester and someone who is not. A typical test consists of yes-or-no questions. The tester begins with some innocuous questions, such as "Is today Tuesday?," and he instructs the subject to answer truthfully to some and falsely to others. Once a pattern of physical responses to true and false answers is established, the tester moves on to the target questions, such as "Have you tried to deceive me today?" The subject is said to "pass" the polygraph if the pattern of his responses to the target questions matches the pattern of his responses to true answers of the innocuous questions; he "fails" if they do not. Nonetheless, some caution is due. Polygraph tests are inadmissible in court, because the same stress responses can be caused by emotions (such as embarrassment) that are unrelated to lying, and because the phrasing of the questions, experience level of the tester and details of how the test was conducted can greatly influence the results. Special Agent Robert Hunter states that the FBI's best polygraphers were assigned to the John Walker case, and he has a high degree of confidence that the results are accurate. See Hunter, 120-121.

[21]Ibid., 118-122.

[22]He served as a radioman onboard the *USS Simon Bolivar* from August 1965 to December 1967 and would have had routine access to all of the cryptographic materials on board, including KW-7 keys and classified manuals. Additionally, the ship's captain is known to have allowed him to see the Single Integrated Operations Plan, which specified

the full details of the US plans for launching a nuclear strike on the Soviet Union and its allies (including air-, land-, and sea-based strikes). See Early, 49-53.

[23]Hunter, 185-186.

[24]Early, 86.

[25]Jerry Whitworth did get the modification work order that had directed an alteration of the KWR-37 and passed it to the Soviets, via John Walker, in November 1980. See Barron, 186.

[26]Ibid., 210.

[27]Yet even this small amount of information, delayed by several weeks, was vital to the US victory at Midway. Specifically, the information gave Admiral Nimitz sufficient advance warning that the Japanese would attempt a submarine cordon so that he could order his ships to sea before it arrived. He also knew that Japanese seaplanes would attempt to refuel from submarines at Frigate Shoals, and so he stationed ships there to prevent it. He knew that there were four carriers in the Japanese task force, which contributed to his decision to rush the *USS Yorktown*'s repairs into a near-miraculous two days, and he knew that the Japanese did not expect her to be in action. The information also indicated that the Japanese attack toward the Aleutians was a feint, and it could be ignored. All of this, plus enormous luck and courage, was critical to the Americans successfully overcoming a major disparity in combat power between the fleets. See Barron, 31.

CHAPTER 4

KEY MANAGEMENT

> They usually had forewarning of the B-52 strikes. Even when the B-52s diverted to secondary targets because of weather, they knew in advance which targets would be hit. Naturally, the foreknowledge diminished the effectiveness of the strikes because they were ready. It was uncanny. We never figured it out.[1]
>
> Theodore Shackley, CIA station chief in Saigon from 1968-1973, quoted in *Breaking the Ring*

Overview of Key Management

Key management describes the methods and policies used to handle key material. This report will focus on two major subcomponents of the FBS key management system. The first is the FBS key distribution plan--how key material was distributed to all of the people and places that needed it. This chapter will show that, while in theory the distribution of key material was tightly restricted on a need-to-know basis, in practice this principle was trumped by the need to ensure that all Navy ships had all the key material they might need for any potential mission worldwide. The second major subcomponent to be studied is the auditing system. This was the main method that the Navy used to ensure that keys were not lost, stolen or mishandled by the personnel who are legitimately issued the keys. While highly elaborate and regarded with significant apprehension by the sailors who had to face them, this report will show that they were totally incapable of detecting illicit copying of the key material, even if the audits had been carried out 100 percent perfectly.[2]

The FBS Key Distribution System

Before beginning to study the key distribution system for FBS, it is worth discussing general design criteria for key distribution. Clearly, the distribution of the key is of primary importance to the overall security of the system. But during the time period under study (1967-1974), there were some fundamental misunderstandings about how to look at security conceptually, which contributed to the weakness of the key management system ultimately implemented for FBS. The most important of these conceptual errors was to focus almost exclusively on securing the communications path, rather than on securing the data itself. Ultimately, what end users want is easy access to, and secure protection of, their data. Likewise, the enemy wants the data; it is irrelevant to him whether it was acquired by a radio intercept, photocopied in a message center, or handed over by its ultimate recipient.

Once a designer focuses on the data, rather than a communications path, it becomes clear that there are two separate design criteria to consider. The first is ensuring that no unauthorized people get access to the data. This is called *data confidentiality*, and it is the feature that most people immediately associate with a communications security system. But good designers also have to take into consideration a second issue: ensuring that every legitimate user who needs the data can get access to it, at the time and place that he needs it. This is called *data availability*. Obviously, these two imperatives conflict to some degree, and the issue calls for a delicate balancing of risks. Yet the fact that there are two separate imperatives was not understood at the time that FBS was designed. Instead, the NSA designers focused almost exclusively on data confidentiality--ensuring that the KW-7 hardware and security policies ensured that intercepted communications

would remain undecipherable to the enemy. If that meant that it was expensive, hard to use, and required extremely restrictive and awkward policy, or if it might lock out legitimate users from time to time, then so be it.

But once the nascent FBS system left the NSA laboratories, the emphasis on security above all changed dramatically. The people who approved the final design of FBS, including the key management architecture--how many different keys were used, how long they were used, how many were issued to ships or stations at a time, who shared keys, and others--were not security experts at all. They were the Navy line officers who commanded the fleet. Although they were unable to put it into words, their actions show that they were far more concerned with data availability rather than data confidentiality. There were two main factors to this mindset: first, there was a genuine ignorance about the real rates of personnel reliability, with commanders grossly underestimating the likelihood of potential problem sailors getting security clearances and access to keys. Second, any ship or station which became isolated by lack of key became an immediate, high-level issue and prompted numerous and vigorous complaints. A key compromise, by contrast, was a totally silent affair for the commander. Thus, commanders were prodded toward approving very insecure systems both by ignorance and by their legitimate concern about leaving ships isolated.

Specifically referring to FBS, recall that the Navy communications architecture system in the mid-1960s to mid-1970s divided the world into four major regions, each with its own NAVCAMS. Within each region, different communications nets used different keys--the submarine fleet used a different key than the surface fleet, for example. This design was both a security feature, given that the enemy acquiring one key

would only compromise part of the entire system, and a logistical convenience feature, in that each NAVCAMS would operate entirely independently of the others.

The problem with this concept is that Navy ships move worldwide. Ships can and do circumnavigate the world, and they do not necessarily know ahead of time where they will be going or when they will get there. There is also no saying whether it will be physically or operationally possible to reach the ship from shore, so there is no guarantee that a ship could be resupplied with keys in a short period of time if it moved into a different NAVCAMS' area unexpectedly. Accordingly, the Navy decided that every ship would be issued with a copy of every possible key that it might need, for every NAVCAMS in the world, for a period well in excess of its planned cruise, just to be sure that no ships became accidentally isolated.

Essentially, the design was based on a series of logical deductions. If the enemy does not get access to the keys, then the KW-7 is secure. If the keys are only issued to trustworthy people, then the enemy will not get the keys. And since cleared people are trustworthy, then the KW-7 system will be secure if the system carefully checked that only cleared people get access to the keys. While this works well as a logic problem, it falls apart in the real world if the assumptions built into it are not true. As was demonstrated in chapter two, the assumption that the clearance process would identify and exclude all potentially untrustworthy individuals is simply wishful thinking. The rest of the logical edifice built on it then collapses.

Consider for a moment the fact that any personnel security system, however well designed, managed and resourced, will have a minimum level of error. That is, even the best system will sometimes allow an untrustworthy person to slip by. It follows that the

risk that any given secret will be revealed to one of these untrustworthy people is simply the rate of error, whatever that might be, times the total number of people who have access to the secret. Chapter two looked at the factors influencing the error rate in the late-1960s and early 1970s; now let us turn our attention to the question of how many people had access to the FBS keys in the same period.

The question is surprisingly hard to answer, and in fact may never be fully known. There was no central list of sailors who were permitted to receive the FBS keys. Essentially, it appears that anyone with a Secret clearance was considered trustworthy enough to handle FBS keys; additionally, every ship commander had the authority to authorize *anyone* onboard his ship to handle classified material, if he thought it prudent and justified by mission needs.[3] During this period, the Navy had around 800 ships in service--the exact number varied as ships moved in and out of dry dock and were commissioned and decommissioned[4]--and each ship would have had somewhere between a handful and several dozen sailors who were assigned to operate the radios and teletypewriters. All of these sailors would have had routine access to FBS keys as part of their daily duties. Communications centers in shore stations were normally even larger than communications sections onboard ships, with scores or hundreds of sailors working in each. Many more sailors worked with key material in other ways, including as couriers and COMSEC equipment repairmen.[5] Thus the minimum number of sailors with routine access to FBS keys as part of their daily duties was measured in tens of thousands--although, again, it appears that no one was keeping a detailed listing of who should have had access, and when, so it is impossible to say exactly. If one adds in the personnel who might have gotten access intermittently, or by fraud or deception, the number may have

been above 100,000.[6] With such a large number of personnel handling the key material, even a very small error rate in clearing personnel with possible security concerns would result in a highly risky system overall.

John Walker's case shows clearly how high those risks actually were. As mentioned before, John Walker was assigned to the supply ship USS *Niagara Falls* in 1971 as she prepared to deploy to the waters off Vietnam. The ship's deployment was planned to be ten months; furthermore, it is believed that the ship had an additional six months of "reserve on board" key as well. Since the ship was a supply ship and had a COMSEC vault on board, it was also used to ferry new key and classified materials to other ships, including submarines and aircraft carriers, and held a large amount of key used for the land forces in Vietnam as well. He was thus able to compromise every key in use in FBS, worldwide, for a period well in excess of one year, in one single delivery before he left. And John Walker remained assigned to the USS *Niagara Falls* for a total of three years (1971-1974). During that period, the quantity of material that he divulged was so large that during his counterintelligence debriefing John Walker was unable to recall precisely all of the things he compromised. He did remember that the Soviets had given him a Minox camera to photograph the key cards, and that he used it so heavily that it wore out. He had to buy a new one to continue his spying.[7]

The FBS Auditing System

The second major part of the key management system to consider was the auditing process. The purpose of audits was to determine whether key material had been handled properly in accordance with policy and regulations. To do this, those who handled key material had to fill out and file forms that detailed exactly when each key

was received, what was done with it, where it was stored, when and where it was loaded into a machine, and when it was destroyed. Some steps, such as the destruction of a key card, required two people to sign off on it; others required the signature of the supervisor of the Classified Materials System (CMS) custodian, or the person overall in charge of the cryptographic materials onboard a ship or in a communications section ashore. Most sailors looked at the whole issue with apprehension, as the documentation was burdensome drudgework--but drudgework that was easy to get wrong and could easily get someone in serious trouble. Many of them, even those in charge of the communications systems, avoided it as much as possible.[8] Yet John Walker was never in any danger of being caught by the audit procedures. Quite the contrary: it is likely that the sheer elaborateness of the audit system was a major help to him in his spying.

Even if they had been executed perfectly, the audit procedures in place were unable to detect what he was doing. All the audit did was to verify that the correct persons signed for the keys at each step, and that they were stored in a correctly configured vault. These restrictions were utterly irrelevant to what John Walker was actually doing--he *was* the "correct person," the CMS custodian, and he did keep them stored in the vault. He was not attempting to steal the key cards outright, or to conceal the fact that he had access to them. Instead, he was making duplicate copies of them--at first, using the photocopier in the vault, and later using a camera. No kind of paperwork would have documented this, and hence no audit of the paperwork would have caught the problem.

But the situation was even worse than useless: it is arguable that the audit system in place actually made his spying easier. He made extensive use of the "mystique" of

COMSEC procedures to keep his superiors from asking questions, and he had a ready-made excuse for spending long hours in the vault by himself, working with classified paperwork. He was the CMS custodian, and he could easily say that he was busy keeping the paperwork up to date. His performance evaluations repeatedly commend him for his deep dedication to keeping the COMSEC account in excellent order and routinely note that he spent quite significant extra hours working in the vault, in fact. And since the procedures for handling classified material were so burdensome, it was easy to convince other people to let him handle their classified materials for them--storing classified materials for them in his vault, serving as a courier between ships and from ship to shore, and signing for extra classified material. However in this way, he was able to take control of classified material that he should not have had access to, simply because it was very convenient for other people to leave it to him to do. One of the many examples of this are the codes used by the US Air Force and US Navy to secure the transmission of the air tasking orders specifying bombing targets in southeast Asia. The USS *Niagara Falls* was a resupply ship and had no direct mission requirement whatsoever for these keys--so how did John Walker get possession of them to compromise them? Simply put, it was easier to leave the material in John Walker's vault for a future rendezvous with an aircraft carrier than to deliver the keys directly from NSA to the carrier every month. The quote from CIA station chief Theodore Shackley at the beginning of this chapter is the result. To be fair to him, it would have been impossible for him to figure out how the missions were compromised. After all, who would have guessed that keys used to secure the transmission of orders to US Air Force B-52s in Guam were being stored on a US Navy resupply ship in the South China Sea, photographed, and passed to the KGB during port

calls in the Phillipines or Hong Kong? When he was recruiting Jerry Whitworth, he emphasized how easy it all was, and how safe--and of course, how good the "bonuses" were when he was able to get additional material.[9]

A larger issue is the question of what is being audited. The FBS audit system checked the chain of custody on the key cards, on the implicit assumption that the key cards were what needed to be guarded. It attempted to exhaustively document who handled them, from their creation to their ultimate destruction, on the assumption, once again, that if only cleared personnel got access to the key cards, then they would be safe from compromise. Using the modern concepts of data confidentiality and availability, however, it is clear that the *data* was what needed to be protected. Control of the paper key cards was important, but only because of the data punched onto them--which means, for example, that having two-man control over the destruction of key cards is irrelevant if there are no controls at all on the photocopier. In fact, focusing on the data, rather than the paper, makes it obvious that there should be no photocopier present in classified spaces.

In summary, when evaluated from the conceptual standpoint of data availability and data confidentiality, it is clear than the FBS key management system was very poorly designed. Far too many people had access to the keys; indeed, it is difficult in retrospect to put an upper limit on how many people might have gotten access to them.

---

[1]Barron, 23.

[2]Key management, as a whole, contains other design criteria as well--for example, the length of time that a particular key is used. As these other criteria had little or no effect on John Walker's compromise of FBS, they will be omitted in this report.

[3]Stilwell, Executive Summary/Key Findings and Recommendations.

[4]When a warship was placed into dry dock for repair and refitting, its COMSEC equipment was removed for safekeeping and it was no longer issued cryptographic key material. Navy ships are typically sent to dry dock for refitting every few years, but the exact timing of when they enter and leave varies considerably. See Bamford, 183-184.

[5]John Walker routinely volunteered both to work as a courier of classified material and to store materials in his vault for other people, in order to copy them for the Soviets. In this way he was able to compromise key material to systems and networks that he would not normally have had any need-to-know or access, such as the cryptographic keys for ground forces' communications nets in Vietnam. See Hunter, 186-188.

[6]The PERSEREC report shows that about one quarter of the Americans convicted of espionage between 1947 and 2001 had no clearance at all when they committed their crimes, so this is not an unrealistic concern. One of the spies without a clearance was Michael Walker, who managed to pilfer over 1,500 classified documents by a variety of subterfuges and taking advantage of security lapses of his superiors. See Herbig, xi and 66; Hunter, 99; Bamford, 219.

[7]Early, *Family of Spies*, 104-106; Hunter, 87.

[8]Barron, 125.

[9]Early, 60-61, 98 and 106-107.

CHAPTER 5

CONCLUSION

> Had we been engaged in any conflict with the Soviets, [the secrets revealed by the Walker ring] could have had the devastating consequences that Ultra had for the Germans.[1]
>
> Secretary of the Navy John F. Lehman, quoted in *Breaking the Ring*

Overview

This report has looked at the factors which went into the design and implementation of FBS during the period 1967-1974. Three main areas were studied: personnel security, technical security, and key management. In all three, the procedures and methods followed to ensure security were starkly inadequate to achieve the results desired--and furthermore, this inadequacy should have been obvious to a contemporary analyst looking for security weaknesses in the system. Unfortunately, there was no one who had the responsibility to look at the system as whole and direct resources intelligently to minimize the overall risk of compromise. Instead, responsibility was divided between organizations and between different people within an organization who were designing and implementing different pieces of the system. It appears that the designers of each subsystem simply assumed that the other parts would be secure and always implemented according to policy; for example, the key distribution system was designed based on the assumption that all cleared personnel would be trustworthy, so the only remaining issue was to prove that only cleared personnel handled the keys.

There is no way to go back in time and undo the mistakes and bad assumptions that led to the compromise of FBS in 1967. It is, however, imperative that these lessons

are applied in the design of future systems and the implementation of current systems. Accordingly, this report advances three main conclusions for security design: designers must have a realistic understanding of what the personnel security system can achieve; they must severely limit the distribution of key material and important technical security information; and they must identify all of their assumptions and actively seek to falsify them.

How Effective Can the Personnel Security System Be?

This report has demonstrated that the personnel security system present in 1967-1974 was unable to detect or respond to even obvious behavioral problems. A large number of changes to the personnel security system were proposed in the wake of the Walker spy ring in 1986-1987, and further study during the intervening years has identified even more proposals. This chapter will not restate them. Suffice it to say that the personnel security system is vital to the overall success of any secure communications system, and secure, reliable communications are fundamental to way that the United States wages war, collects intelligence, and performs most government functions. This report will take it for granted that there should be continuous efforts to improve the effectiveness of the personnel security system.

Yet as mentioned before, no system that deals with human beings will ever reach 100 percent effectiveness--there will always be people who should not get access to classified materials that will slip by. Investigators and commanders will make mistakes. But is it possible to get some general idea of what the level of error might be? To get a direct answer to that question, we would have to know the total number of personnel with security clearances and the total number of those personnel who are spies. Those numbers

are obviously not available, as we will never achieve a 100 percent capture and conviction rate for spies; indeed, there is little information available to know even approximately what percentage of spies are eventually caught and convicted.[2] There are two things which give us some hints about the level of success that might be achieved, however: the success rate of investigations into other questionable behavior, and the rates in the general population of questionable behavior compared to the approval rates for security clearances.

The personnel security system depends on background investigations to weed out potentially unreliable individuals. Since one can assume that the subject of the investigation will actively try to hide indicators of unreliability, the key measure of effectiveness is the investigation's ability to detect behavior or traits that the subject wants to keep hidden. One good historical example of such investigations is the search for homosexuals at NSA during the 1960s. Recall that the NSA conducted a major operation to root out homosexuals in the early and mid-1960s in response to the defection of two homosexual employees. In response, the NSA made inquiries on an employee's sexual proclivities a major part of the personnel security system. As a component of both the application process and periodic security reinvestigations, all employees were given polygraph tests with an "embarrassing personal questions" section, to determine if they were at risk of blackmail. In it, they were explicitly asked if they had had any same-sex sexual contact after age 18. Investigators were also required to ask co-workers, friends, and family members about the subject's sexual behavior and to submit a formal evaluation of whether the subject might be homosexual.[3]

So how effective was this all-out attempt to eliminate homosexuals from NSA? To answer this question, we must first determine how many total employees worked at the NSA. The exact number of employees at the NSA is classified, but James Bamford estimates the number at more than 70,000 during the 1960s.[4] Then we must estimate the prevalence of homosexuality among those 70,000 people. That is a complicated question to answer, largely because it is difficult to come to a single definition of homosexuality--as distinct from bisexuality, experimentation, or self-perception of sexual orientation, for example. Since the NSA investigators were asking about sexual behavior, let us consider solely the question of how prevalent same-sex sexual behavior is in the general population. One of the largest scientific studies which researched this was the National Health and Social Life survey, conducted by the National Opinion Research Center at the University of Chicago in 1992. According to this study, 2.7 percent of American men report sexual contact with another man in the last year, and 4.9 percent reported sexual contact with another man after age 18.[5] This level of incidence would translate to about 1,900 employees with same-sex sexual contacts within the past year and 3,400 employees with same-sex sexual contacts since age 18. Yet the multiyear investigation resulted in only 26 personnel being identified as homosexual and either fired or forced to resign.[6] Thus, even using polygraphs and professional investigators, the system was able to identify between 0.5 percent and 1.5 percent of the people for whom it was searching.

Another hint about what kind of results one can expect from the personnel security system is to look at the rates of questionable behavior in the general population, as compared to the rejection rate for security clearances. Currently, security clearances are granted or withheld based on the *Adjudicative Guidelines for Determining Eligibility*

for Access to Classified Information, which became effective in 1997. This document identifies 13 general areas of concern that could be the basis for denial of a security clearance: alcohol consumption; disloyalty to the United States; criminal conduct; drug involvement; emotional, mental and personality disorders; financial considerations; foreign influence; foreign preference; misuse of information technology systems; outside activities; personal misconduct; security violations; and sexual behavior. Dr. Herbig and Dr. Wiskoff note that about 80 percent of the Americans convicted of espionage or attempted espionage from 1947-2001 exhibited signs of violating one or more of these guidelines. However, they also note that there are no comparable statistics to show what the prevalence of such questionable behavior is in the general population--these are very broad categories, and it may well be that large minorities, or even majorities, of the individuals in sensitive positions exhibit one or more of them. For example, they cite the case of Jonathan Pollard, whose strong commitment to the well being of the state of Israel induced him to pass classified information to the Israelis. Yet they note that such concern for Israel is common among American Jewish households, but has apparently only been a factor in one case of espionage.[7] Likewise, misuse of information technology is a very broad area and can include relatively common violations of security policy, such as writing down passwords.

One further example is the case of mental illness, which is clearly an area of concern under the *Adjudicative Guidelines*. According to *Mental Health: A Report of the Surgeon General*, 19 percent of the general population of the United States has a diagnosable mental illness, 6 percent have an addictive disorder, and 3 percent have both a mental illness and an addictive disorder. Most of the sufferers continue to function

more-or-less well outwardly, despite the internal turmoil: only between a third and a quarter of these illnesses result in diagnosable functional impairment or are severe enough to interfere with social functioning. The others may or may not be detectable by an untrained observer, even though they can seriously compromise the sufferer's judgment and ability to comply with security policy.[8] Note also that some of these diseases are episodic--for example, an individual becomes clinically depressed following a divorce--which might not be present at all during the individual's security background investigation. As has been documented in chapter two, co-workers and supervisors are reluctant to report someone who is going through a major life difficulty as a security risk, for fear of making a bad situation worse. Yet such episodic emotional or mental problems can be a major indicator of security risk.[9]

One can conclude that the rates of problematic behavior and security risk indicators are relatively high in the general population. Even assuming that these rates are significantly lower among personnel submitted for security clearances, the overall numbers can remain quite high. For example, even if the rate of alcohol and substance abuse is 99 percent lower among the cleared population than the general population, it would still indicate that about one in 1,000 clearance-holders has an active substance abuse problem at any given time. Note further that, first, a 99 percent effectiveness rate in weeding out substance abuse is highly unlikely given what we have seen about the lack of success in weeding out homosexuals, and second, substance abuse is only one possible security problem. One must conclude that the personnel security system, while vital, will never be able to screen out many personnel exhibiting security risks, and the rest of the security system must be designed with this in view.

What Can Key Management and Auditing Achieve?

Based on the previous discussion of personnel reliability rates, what can one say about the design of a key management and auditing system?

The first obvious conclusion is that the distribution of the keys must be tightly restricted. The minimum level of objectionable behavior among even cleared individuals requires it. Planners must assume that, once the number of people who have knowledge of a particular secret--whatever it might be--exceeds a few hundred to a few thousand, then one or more highly questionable people will get access to it. Military commanders throughout history have known this fact and exploited it by, for example, restricting knowledge of an upcoming operation to a very small group of planners; or alternately, by deliberately involving a large number of personnel in a planning process, with the intent to deceive the enemy. The same timeless principle applies to key material and cryptographic information as well. The FBS system, with tens or hundreds of thousands of sailors handling the keys, was inherently insecure and unsecurable. Future systems must be designed differently.

A related issue is that designers must be realistic about what an audit can and cannot do. What system managers truly want to audit is *data*: they want to determine who has gotten access to the classified data. The trouble with this is that it is for practical purposes impossible, because one cannot effectively rule out duplication. John Walker duplicated keys with a camera or photocopier; modern systems use electronic keys, which can be duplicated any number of times easily and without any trace whatsoever. The auditor will not have direct access to the most important information and will be forced to rely on the proxy information of who has entered a particular secured area or

signed out a particular keying device. An analogy with the more familiar world of financial audits is instructive: it is as if a financial auditor was unable to count the actual money and instead was forced to rely on details of who entered a store and who was operating the cash register at the time. Few people would put much faith in the ability of such a system to prevent embezzlement or theft; yet this is exactly the position that the cryptographic audits are in. Indeed, there is little evidence that cryptographic audits were ever instrumental in identifying a case of espionage; at best, they seem to have been useful in developing damage reports or as supplemental evidence once a person is already under investigation as a spy. So while they are certainly necessary, audits are in no way sufficient to ensure that keys are not mishandled or duplicated.

How Should One Handle Assumptions?

Perhaps more than anything else, the Walker spy case is a study in assumptions. Time and again, individuals made decisions based on assumptions that proved to be woefully incorrect. In many cases, these assumptions were based on nothing more than wishful thinking, or on the fact that it would be very convenient if certain things were true. There is little or no evidence that decision makers attempted to verify or falsify them, even when such an attempt would be easy to make. For example, there was no attempt to verify whether or not the policies written at NSA were being implemented as specified in the fleet, or even to verify if the policies *could* be implemented with the time, resources and personnel available.

Another military truism is that successful planners must clearly distinguish between facts and assumptions. All real-world plans will require some assumptions, as information will never be perfect. However, a successful planner will then try to verify or

falsify his assumptions, continuing to do so until successful--either proving the assumption true, making it into a fact, or proving it false. Much of the technical security built into the KW-7 and its key management plan relied on a series of assumptions which were highly unlikely to be met in practice. Some of those assumptions were never shared with critical decision makers or the personnel who had to implement the solution; many of these assumptions were simply wrong, and would have been identified as such if any follow-up investigation had been done.

Conclusion

One of the most startling facts about the John Walker spy case is that there was ample evidence available at the time to indicate that a serious breach of communications security had occurred. Navy intelligence officers noticed a number of worrying indicators, beginning in the early 1970s. Soviet Navy submarines suddenly got dramatically quieter and developed an ability to stay just outside the effective range of US sonobuoys--exactly as if they knew the full details how the US was detecting them. They also started showing up outside US submarine bases just before American submarines were scheduled to put to sea. The Soviet Navy showed an uncanny ability to get intelligence collection ships at the right place and time to capture data from fleet exercises. “It was as if they had a copy of the OpPlans [operational plans] or something,” one frustrated admiral said at the time.[10]

We now know that they did, in fact, have a copy of the OpPlans--and everything else of any importance to the US Navy, for a period of almost twenty years. Richard Haver, the deputy director of Naval Intelligence, said that they had wondered at the time if there was a communications security breach, but there was no proof. Even in

retrospect, it is not clear how they could have gotten such proof. The design of FBS was such that, even if a Soviet spy had brought verbatim copies of FBS intercepts to the CIA, it would have been impossible to produce a comprehensive list of potential suspects, even a list that was tens of thousands of names long.

And that fact was the fundamental problem with the system design of FBS: that the system in place at the time depended on perfect awareness and flawless execution by thousands of people, over the course of decades, around the world--any lack in any area could (and did) cause catastrophic failure of the entire system. That the system was deeply flawed should not be surprising, since FBS was not in fact designed as a system at all. Each component and subsystem was designed in isolation and based on a series of assumptions. No one had overall responsibility for verifying whether the assumptions were realistic, or even for ensuring that the designers of other subsystems and the Navy chain of command were aware of them. Decision makers did not have the information that they needed to make good choices about resourcing, risk assessment, and operational methods and procedures; they made their decisions based on what they did know, and that resulted in a system that was far more unsafe than anyone realized.

It is all very well to look back at the period 1968-1974 and criticize the poor judgment and bad decisions of the individuals involved. Yet this report has demonstrated that the security system as a whole was so poorly designed that it virtually guaranteed bad choices would be made at every level--from the admirals and senior executives responsible for adequately funding the security system without having a full understanding of the dangers being run, to the engineers designing equipment in isolation from the real day-to-day constraints faced in the fleet; from the investigators, who had no

hard, trustworthy evidence of what to look for and hopelessly inadequate tools to uncover critical information, to the first-line supervisors who were expected to spot and stop potential spies without the benefit of training or clear guidance--and while simultaneously maintaining 100 percent operational readiness.

Well-designed systems must take into account the actual conditions and characteristics of its subcomponents. In the case of a communications security system, such as FBS, some of those “subcomponents” are human beings, with all of their foibles and failings. From a design standpoint, it is just as wrong to assume that all of the people involved will execute policy flawlessly as it would be to assume that a mechanical part will never fail. Just as good design involves finding out how the encryptor behaves as the battery loses its charge or the device gets splashed with water, so also good system design should take into account what happens when the operators do not behave as they ought to--whether through malice, carelessness, or simple inability to carry out the requirements with the resources available. The latter two cases can be minimized or even eliminated through better design: that is, the designer must make it as easy as possible to do the right thing and as hard as possible to do the wrong thing. This needs to be an iterative process, based on close observation of what ordinary sailors actually do during fleet deployments, and incorporating improvements and innovations as they become available.

But how does good design address intentional violations? In this case, there are two main issues. First, the operational chain of command must be made thoroughly aware that deliberate compromise is an unavoidable risk, and that that risk rises exponentially with the number of personnel who have access to the transmission. (This means that common-use channels with shared keys, such as FBS was, are effectively impossible to

protect against this threat.) They must also be aware that this risk *cannot* be eliminated, even by the best personnel security system, and that the rate of security relevant misbehavior in the cleared population is relatively high and will remain so under any reasonable set of assumptions. Second, a primary focus of the security system should be actively and continuously seeking evidence of the compromise of a given communications system. These two elements can only be satisfied if the individuals who have access to a particular item--such as a cryptographic key, or an OpPlan--are identified *by name* ahead of time. While that sounds very burdensome, it is in fact common procedure for the distribution of paper copies of sensitive documents, such as war plans, to be restricted to those individuals named on such a short list. Such constraints are essential, since it is impossible to do any sort of forensic analysis if a compromise is suspected without some list of possible suspects. Alternately, if the operational command decides that such restraints are not possible, it needs to be clearly understood that the data in question is at a high, and possibly extreme, risk of compromise.

Military operations always involve a measure of risk. There is no way to completely eliminate the risk of a rogue insider betraying his country. As mentioned at the beginning of this report, there have always been, and there will always be, pathologically greedy people in any organization as large as the US Navy. The important point to draw from this analysis of the John Walker spy case is that commanders must be aware of those risks, minimize them as much as feasible with coherent, well designed security systems and operational plans, and seek continuous improvement in the field.

[1]Barron, 212.

[2]A good historical example of this is the Soviet espionage efforts before and during World War II. After the collapse of the Soviet Union and large-scale declassification of signal intercepts now shows that there were several hundred spies active in the United States; however, only a small handful were detected at the time, and fewer than a dozen were tried and convicted of espionage. See Herbig, x.

[3]Bamford, 107.

[4]Ibid., 4.

[5]The equivalent percentages for women were 1.3 percent within the last year and 4.1 percent since age 18. However, since both the U.S. Navy and the NSA were almost entirely male during the 1960s, this report will only use the data for American men. See the National Opinion Research Center, University of Chicago, The National Health and Social Life Survey ("The Sex Survey") Summary, (posting date unavailable, study data collected in 1992); available from http://cloud9.norc.uchicago.edu/faqs/sex.htm; Internet.

[6]Bamford, 149.

[7]Note also that, if 80 percent of the convicted spies exhibited one or more questionable behaviors or traits, then conversely one in five spies exhibited no reason for suspicion at all. See Herbig, 52-55.

[8]United States Surgeon General, *Mental Health: A Report of the Surgeon General*, (date unavailable); available from http://www.surgeongeneral.gov/library/mentalhealth/chapter2/sec2_1.html, Epidemiology of Mental Illness; Internet.

[9]Dr. Herbig and Dr. Wiskoff found that 27 percent of convicted spies began their espionage in the wake of a major life trauma, such as divorce, death of a loved one, or extramarital affair. See Herbig, 55.

[10]Barron, 22-25.

GLOSSARY

COMSEC. Communications Security.

Cryptologic. The mathematical algorithm used by an encryptor to determine which character will substitute for another.

Keystream. A stream of pseudorandom characters that is generated by the encryptor. The message is encrypted by mixing the keystream and the unencrypted message.

Personnel Security. Policies and procedures which govern who is given (legitimate) access to classified information.

Physical security. Measures taken to ensure the physical control of the areas where classified material is stored, and control of physical access to the encryptors and their associated information and equipment.

Technical security. The security features designed into COMSEC devices that make recovering classified data from the transmitted message impossible for anyone except the legitimate recipient. This report specifically addresses only the technical security measures taken for the KW-7 encryptor.

BIBLIOGRAPHY

American Psychiatric Association, “Position Statement on Homosexuality and Civil Rights,” *American Journal of Psychiatry, 131 (4),* (15 December 1973), 497.

Andrew, Christopher and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB.* New York: Basic Books, 1999.

Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency.* Boston: Houghton Mifflin, 1982.

Barron, John. *Breaking the Ring.* Boston: Houghton-Mifflin, 1987.

Bucher, Lloyd M. *Bucher: My Story.* New York: Doubleday & Co., 1970.

Earley, Pete. *Family of Spies: Inside the John Walker Spy Ring.* New York: Bantam Books, 1988.

Herbig, Katherine L. and Martin F. Wiskoff, Defense Personnel Security Research Center. *Espionage Against the United States by American Citizens 1947-2001,* PERSEREC Technical Report 02-5, July 2002.

Hunter, Robert W. and Lynn Dean Hunter. S*py Hunter: Inside the FBI Investigation of the Walter Espionage Case.* Annapolis, Maryland: Naval Institute Press, 1999.

Kahn, David. *The Code Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* 2d ed. New York: Scribner, 1996.

Kalugin, Oleg and Fen Montaigne. *The First Directorate.* New York: St. Martin’s Press, 1994.

Lerner, Mitchell B. *The Pueblo Incident.* Lawrence, Kansas: University Press of Kansas, 2002.

National Opinion Research Center, University of Chicago, *The National Health and Social Life Survey ("The Sex Survey") Summary*, (posting date unavailable, study data collected in 1992); available from http://cloud9.norc.uchicago.edu/faqs/sex.htm; Internet

Stilwell, Richard G., General, USA, Ret. (Chairman). *Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Policy and Practices.* Delivered to the Secretary of Defense on 19 Nov 85. Downloaded from http://www.fas.org/sgp/library/stilwell.html.

United States General Accounting Office, *Security Clearances: Consideration of Sexual Orientation in the Clearance Process.* Report to Congressional Requesters,

GAO/NSIAD-95-21, 24 March 1995, 1-3 and 9-10.

United States Surgeon General, *Mental Health: A Report of the Surgeon General*, (date unavailable). Downloaded from http://www.surgeongeneral.gov/library/mentalhealth/chapter2/sec2_1.html.

Walker, Laura and Jerry Horner. Daughter of Deceit: The Human Drama Behind the Walker Spy Case. Dallas: Word Publishing, 1988.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Dr. Donald P. Wright
CSI
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

Mr. Kendall D. Gott
CSI
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

CDR Brett W. Wiseman
Department
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 17 June 2005

2. Thesis Author: Laura Heath

3. Thesis Title: An Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967-1974, as Exploited by CWO John Walker

4. Thesis Committee Members: _____

Signatures: _____

_____

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
Direct Military Support (10)	/	Chapter 3	/	12
Critical Technology (3)	/	Section 4	/	31
Administrative Operational Use (7)	/	Chapter 2	/	13-32

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
	/		/	
	/		/	
	/		/	
	/		/	
	/		/	

7. MMAS Thesis Author's Signature: _____

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).