with A5, the office of Soviet cipher systems. Pelton had, in fact, written the manual describing those systems. He had served as a staff member on the Wagner Committee, which had worked on plans for Bauded Signals Upgrade. Given his grade level (GS-12), it was hard to imagine a more damaging defector.[23]

(U) Pelton possessed a nearly photographic memory and a gift of gab which marked him as a rising star in A5. But unknown to his management chain, he had also been operating on the margins of financial ruin. In the early 1970s he decided to house his family in surroundings more appropriate to his idea of his status. Without proper funding, he began building a large house on a five-acre tract in rural Howard County, Maryland, doing the work himself as he could scrounge the materials. Meanwhile, his family lived in squalor, awaiting the grand dwelling. But Pelton soon ran into financial difficulty, and in April of 1979 he filed for bankruptcy. He resigned from NSA the following July, evidently to improve his financial condition. Outside of NSA, Pelton failed at everything he tried, andwithout a regular paycheck his condition sank further. He tried marketing a product that was supposed to improve automobile gas mileage, but it didn't work, and he drifted from job to job in retail sales.[24]
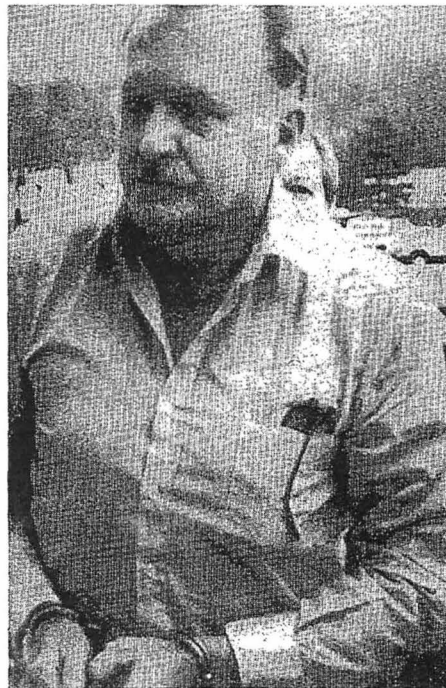
(U) **Ronald Pelton**

(U) On October 23, 1985, just three days after his voice was identified on the tape, the FBI found Pelton living in an apartment in downtown Washington and working as a boat and RV salesman for Safford Yacht Sales in Annapolis. Previously religious and abstemious, he had undergone a complete personality change. He and his wife since 1961 were divorced, and Pelton was living with another woman. Financially, Pelton was doing better than at any time since his resignation from NSA, but the FBI quickly discovered that the two drank heavily and were deeply into drugs. They could be observed on frequent drug buys.[25] The FBI initiated twenty-four-hour surveillance.

(U) Yurchenko's information was old, and no one was sure if Pelton was still passing information to the Soviets. Then on November 4 Yurchenko redefected to the Soviet Union, and the FBI lost its only witness, were they to arrest Pelton and bring him to trial. Not only had they lost Yurchenko, but they had recently let former CIA agent and Soviet spy Edward Lee Howard slip through surveillance to escape to the USSR. With

Yurchenko and Howard gone, could Pelton be far behind? The FBI threw a virtual blanket over Pelton – at one point over 200 agents were involved in the surveillance.[26]

(U) David Faulkner, the FBI agent in charge of the case, was afraid Pelton would flee the country, but had no evidence to hold him, unless Pelton himself gave it to them. Wiretaps (authorized by the Foreign Intelligence Surveillance Court) showed that Pelton and his girlfriend, Ann Barry, were into alcohol and drugs, and FBI investigations showed that he had embezzled $50,000 from the yacht sales company where he worked. But there was no evidence of contact with the USSR. So Faulkner, after a thorough workup on Pelton's character and personality, decided on a risky strategy. He rented rooms at the Annapolis Hilton and set one of them up as an interrogation room for him, Pelton, and a second agent Dudley "Butch" Hodgson. Then, at 0930 on Sunday, November 24, Faulkner called Pelton, who was at the yacht company office, identified himself, and asked Pelton to come to the hotel to talk to him on a matter of "extreme urgency" involving sensitive national security.

(U) Once Pelton was in the room, Faulkner proceeded to detail the life of a hypothetical person, who clearly was Pelton himself. The two FBI agents also played the tape of the phone calls to the Soviet embassy in 1980. Pelton immediately understood that the FBI knew all about his espionage, but seemed to think that they wanted him to become a double agent. So, declining the offer to have a lawyer present, he proceeded to try to talk his way out of it, admitting obliquely that the person that Faulkner and Hodgson sketched was really himself. He admitted a lot – contacts with Soviets, trips to Vienna, payments of $35,000 plus expense money, all to secure the FBI's "cooperation." [27]

(U) By the end of the interview, Pelton so trusted the two agents that he gave up his passport to them and was permitted to go back to his apartment in Washington. But that evening Faulkner again called Pelton, who was by this time at the apartment, and asked him to come back for more questions. During this second interrogation in Annapolis, Pelton placed an X on a map showing where the undersea cable tap was. (His mark was off by a considerable distance.) Once Pelton admitted that what he had done would damage the United States (a key element in the evidentiary chain), Faulkner and Hodgson gave Pelton a waiver of rights, which he signed. Once they had his signature, they arrested him.[28]

(U) Pelton's "confession" told the FBI that he had several contacts with the Soviets in Washington and had met KGB interrogators at the Soviet embassy in Vienna, Austria, twice: once in 1980 and once in 1983. A third trip was planned in October of 1985, but Pelton missed his contact in Virginia in September, and made no further contact with the Soviets. In fact, by the time of his arrest he was trying to avoid them.[29]

(TS//SI-UMBRA) His first Vienna meeting had been very thorough, consisting of some forty-four hours of debriefing, but it was conducted by people who had no expertise in cryptology and was less productive. The 1983 meeting was conducted by a KGB handler who, although not an expert in cryptology, was highly skilled at interrogation. This time there was very little that Pelton did not tell them about his job. He laid out the entire NSA

25X1

(U) Throughout, Pelton had been unhappy with the amount of his KGB payments, and he tried to drop contact following each meeting. He initially demanded $400,000, but in the end settled for $35,000 spread over five years. For him, spying was not very lucrative.[30]

(U) Ronald Pelton was the first spy that NSA took to court. In pretrial negotiations NSA worked gingerly toward a plea bargain, which was how all previous espionage cases had been resolved. But Pelton's defense lawyer, Fred Warren Bennett (who had also defended John Walker earlier in the year; see page 420) advised Pelton to hang tough and go to trial. Bennett expected that the "confession," consisting of unrecorded admissions to two FBI agents in a hotel room, would be thrown out. Without it, the government didn't have a case.[31]

(TS//SI) The trial was scheduled to begin on May 27, 1986. Preparations were lengthy and elaborate. The government had to establish the sensitivity and fragility of SIGINT, and had to reveal in open court SIGINT of value that Pelton had revealed to the Soviets. The Agency decided to put William Crowell, the chief of A Group, on the stand to tell the jury about SIGINT. The "SIGINT of value" would be the Ivy Bells project. The FBI had the map that Pelton had used to designate the undersea tap. Crowell would have to reveal to the jury that the Soviet Union was a SIGINT target (a first admission) and would have to produce the map showing the location

(U) William Crowell

that Pelton had designated to the Soviets. After the introductory course on SIGINT, the revelation of the project would be dramatic enough to convince them of the seriousness of Pelton's espionage. The Agency was determined, at all costs, to hold the line at that point – nothing further on Ivy Bells, nothing about the intercept systems used against the Soviet targets, and certainly nothing about the attack on Soviet cipher systems. It was a risky strategy that could easily have led to the revelation of more sensitive information in open

court. The very idea of having someone as knowledgeable as Crowell testify in open court sparked controversy within NSA. The director, General Odom, issued a memo to all personnel explaining that the information revealed at trial would be a one-time affair and that classification guidelines would not be changed as a result.[32]

(U) The strategy worked. The judge allowed FBI agents to testify about Pelton's admissions in the hotel room, even though they did not amount to a signed confession. Crowell's testimony and cross-examination did not result in damaging revelations beyond those already agreed upon. In the end, the jury convicted Pelton on four of the six counts. Sentencing was left to the judge.[33]

(U//FOUO) The trial was followed by a long interval before sentencing, agreed to in order to debrief Pelton on what he had told the Soviets. The carrot was the sentence: if he cooperated, the government would ask for a lighter sentence. The debriefing was done in a

PL 86-36/50 USC 3605

It lasted from July to December, and was excruciating. Without documents, it was a matter of dredging through Pelton's memory. At one point the interrogators employed a virtual hypnosis technique to get him to recall as much as possible. In the early stages, Pelton lied, but when confronted with the results of a polygraph showing deception, he eventually made a clean breast of things. NSA came away with information that it would never have thought to ask Pelton. One of the most jolting was the revelation that, before going to the Soviets, Pelton had tried to sell his wares to muckraking journalist Jack Anderson. Anderson took the information and published it, but never paid Pelton. Desperate for cash, Pelton then decided to contact the Soviets.

(U) At the sentencing, the FBI indicated that Pelton had cooperated. But it wasn't sufficient. An outraged judge gave him the maximum sentence on all counts – three consecutive life terms plus ten years.[34] He was remanded to Lewisburg Penitentiary in Pennsylvania.

(TS//SI-UMBRA) Ronald Pelton was the most damaging cryptologic spy since William Weisband in the 1940s. He handed the Soviets everything he knew about the NSA attack

25X1

In his classified declaration prior to trial, General Odom said, "Disclosure...provides the Soviet Union with a virtual tutorial on U.S. signals intelligence capabilities 25X1

25X1

25X1

It was a devastating blow, far exceeding anything that other, more famous spies like Aldrich Ames later gave to the Soviets.

(U//FOUO) But to the public Pelton was a minor spy, and today few Americans even remember who he was. This curious twist resulted partly from Pelton's own personality. He came across as a buffoon – haggard, stubbly chin, hang-dog expression. The press constantly referred to him as a minor functionary at a relatively low salary level, as if this somehow separated him from truly sensitive information. NSA's trial strategy worked to perfection, revealing just enough to convict without getting into the avalanche of more sensitive material that he also sold to the Soviets. The real story of the Pelton incident was the amount of information that did not come out.[36]

(U) Benjamin Bradlee

(U) The Pelton trial eventually became notorious for a sideshow – the Ivy Bells incident. This bizarre story overshadowed the trial itself, and became a cause célèbre on the issue of First Amendment rights.

(U) It began in December of 1985, soon after Pelton was arraigned in federal court in Baltimore. An alert newspaper reporter heard the name "Ivy Bells" being introduced by the defense lawyer, and it appeared in the newspapers the next day. An even more alert *Washington Post* reporter, Bob Woodward, picked up the reference and went to his editor, Benjamin Bradlee, with a proposal that the *Post* publish a story on Ivy Bells, an operation that Woodward had been tracking for years through his collection of various bits of journalistic exposé. But instead of approving the article for publication, Bradlee called the federal government.

(TS//SI-UMBRA) The first meeting took place in the offices of the intelligence community staff on F Street in downtown Washington, on December 5. Bradlee attended, in company with Len Downie (the managing editor) and his lawyers. The principal for the government was General Odom, along with his own lawyer, Elizabeth Rindskopf, and the director of naval intelligence, Admiral Richard Haver. Bradlee outlined the story that Woodward had put together, and said that, since Pelton had told the Soviets all about the cable tapping operation, he could see no damage to national security. Odom replied that many aspects of the operation were not known to the Soviets and that publication could result in severe damage to national security. Bradlee scoffed at this and gave to the government team a synopsis of previous publications relating to this very program and similar underwater SIGINT operations, beginning with a *New York Times* article by Seymour Hersh in 1975, during the Church and Pike Committee hearings. Admiral Haver later summarized Bradlee's charge: "All of this indicates that the security of very

sensitive information with the U.S. government is very poor, a fact that Mr. Bradlee finds most disturbing." But Rindskopf assured the *Post* that NSA did not intend to use Ivy Bells at trial except in a very general sense, and Bradlee agreed to withhold publication, at least until he could examine the trial transcript to see how much information the government revealed. Odom remarked later about Bradlee that "I found his behavior in that situation beyond reproach." And so the immediate threat receded.[37]

(U) But the story "had legs," as journalists like to say. The next April, with trial about to begin, Woodward put together a story on the Ivy Bells operation that would run concurrent with the trial. Scheduled to run on May 4, its publication was once again delayed after William Casey called Bradlee to protest. On the tenth, Ronald Reagan called *Post* publisher Katharine Graham, urging that portions of the article be deleted in the interest of national security. But he added ominously that, if the *Post* did not police itself, the Department of Justice might initiate prosecution under Section 798 of the criminal statute.

(U) The issue remained secret until later in May, when NBC released a rather general story on Ivy Bells. Casey stated publicly that he was considering recommending prosecution of NBC under Section 798. But with the story already out, the *Post* decided the time was ripe for its own story. A newspaper that had published *The Pentagon Papers* and the Watergate story, both under threat of retaliation by the Nixon administration, was not likely to back down in this case, but Bradlee ultimately agreed to delete details of the story. He later said that fear of prosecution did not faze him, but national security did. "In my heart, I think the Russians already know what we kept out of the story. But I'm not absolutely sure of that."[38]

(U) Once again, Casey went to Justice with a request to prosecute and issued a public warning to news organizations not to publish "speculation" on sensitive national security issues. The warning related to material that was being revealed in the Pelton trial. But the DCI was out on his own limb. Justice Department lawyers were notoriously reluctant to prosecute news organizations in situations where first amendment rights could be at issue. In this case, they openly scoffed at the idea of prosecuting for "speculation."[39]

(U) The Pelton trial occurred at the tail end of military operations against Libya resulting from the La Belle Discoteque bombing. Government leaks in that case led to threats by Casey and NSA director Odom to prosecute news organizations that published the leaks (see page 359). It also led the Reagan administration to threaten to polygraph everyone with access to "sensitive intelligence" (read primarily SIGINT), a threat that was derailed when Secretary of State George Shultz threatened to resign if anyone from his department were confronted with a demand to be polygraphed.[40] Senator David Durenburger of the SSCI examined the issue from both sides and cast a pox on both houses. The Reagan administration had been a notedly leaky ship and had to tighten up if it were to have any credibility in the courtroom when prosecuting news organizations. But, on the other hand, news media seemed to have taken the wraps off. "...for whatever reason, there is a growing sense that there is nothing which is not fair game."[41]
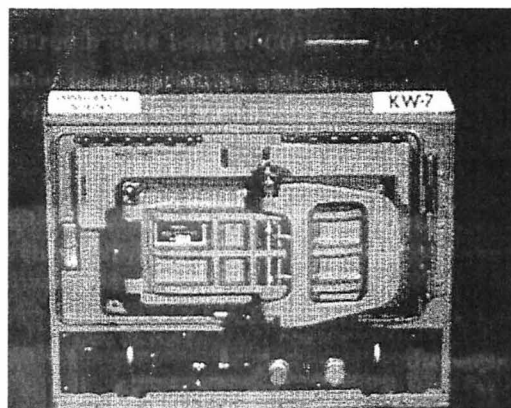
(U) WALKER

(S) In the late 1960s, the KGB created a new organization. Called the Sixteenth Department of the First Chief Directorate (foreign intelligence), it was set up specifically to recruit and handle foreign code clerks who could provide cryptographic information. NSA received information that the organization had twenty agents working full time on North Americans alone.

(S) This could only mean that the Soviets had succeeded in recruiting Americans with access to cryptographic key and that U.S. military communications could no longer be considered secure. A high-level NSA study chaired by the head of COMSEC, David Boak, concluded that crypto key was highly vulnerable to compromise and that every effort should be put into better key security. At the time, NSA did not even know about John Walker.[42]

(S) The findings of the Boak Committee dovetailed with other concerns about the intrinsic insecurity of naval communications. The U.S. Navy relied for communications security largely on a single device, the KW-7, and its sister, the KW-37. First deployed in 1963, the KW-7 was used to secure ship-to-shore, ship-to-ship and shore-to-ship communications throughout the Navy. The KW-37 was used in a broadcast mode for information that went to the entire fleet. NSA's concern was with over-use. The circuits involved transmitted information in staggering volumes, yet the Navy had established only two basic nets – the Atlantic and the Pacific. NSA discovered that when use exceeded a certain volume, the KW-7 and KW-37 could be vulnerable to cryptanalytic attack. To their horror, the COMSEC people at NSA found that the Navy routinely exceeded that volume by a factor of six. The information about the Sixteenth Department heightened the concern – its effort made no sense if they were not exploiting. NSA became very concerned about security of the circuits secured by the KW-7 and KW-37.[43]

(U) KW-7

(S) Fearing that the Navy would never change the employment of the KW-7, COMSEC technicians began designing a drop-in board that would protect the device even when used in the current volumes. They still didn't know about John Walker.[44]

(U) In November of 1984, one Barbara Walker, then living in Maine, contacted the FBI about her ex-husband, John A. Walker, who was living in Virginia. John, she alleged, was a spy. Barbara Walker was an admitted alcoholic, and the FBI initially did nothing about her charges. But agents in the Norfolk office took her charges more seriously, and retrieved Walker's personnel file from the Navy. It was written in almost unintelligible

Navy personnel language, and they needed an interpreter. The agent in charge of counterintelligence investigations in Norfolk had recently collaborated with a threat analysis office in NSA's COMSEC organization. He called his contacts at NSA and asked them to look at the Walker file. NSA's conclusion that, if Walker were a spy, the United States had a big problem. John Walker had had access to a huge number of cryptographic keys and equipments.

(U) The Bureau opened a full field investigation and got a court order to tap his phones. For some weeks it seemed that they were running aground, but then he began talking about an important meeting in the Washington suburbs. On the assumption that he would be going to a dead drop, the FBI deployed a huge tracking team.

(U) John Walker (on left)
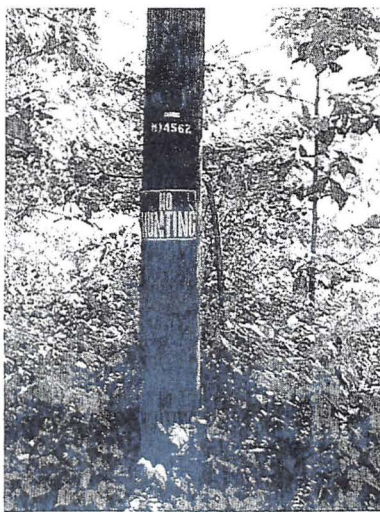
(U) Drop point

(U) On May 19, Walker drove north on I-95 to the Maryland suburbs of Washington. Once there, he proceeded along a serpentine route that had him driving to and fro for hours (the FBI estimated that the full route would have taken four hours) to the drop location on a country road outside of Poolesville, Maryland. There, just after 8:30 in the evening, by a telephone pole with a "No Hunting" sign on it, he deposited a package containing classified material. The FBI swooped down and picked it up as soon as he was out of sight. But when he proceeded to the Soviet drop location, there was no package there (which would have contained the Soviet payments for Walker's previous drop material). Puzzled, he drove back to his own drop location, which was the alternate location for the Soviet material. He found neither the Soviet payment nor the package he had so recently deposited there. He drove back and forth between the two locations several times, checking and rechecking. Then, puzzled and suspicious, he returned to his motel, a Ramada Inn in Rockville, Maryland, which he reached just before midnight.[45]

(U) At 3:30 A.M., an FBI agent posing as a motel desk clerk phoned Walker's room to tell him that his car had been hit and damaged and that he was needed downstairs. As Walker left the room he was confronted by two FBI agents. In the confrontation, all three drew their weapons – Walker dropped his first. The Bureau had just bagged the most damaging spy in American history.[46]

(U) KGB agent's map for Walker

(U) Detailed map
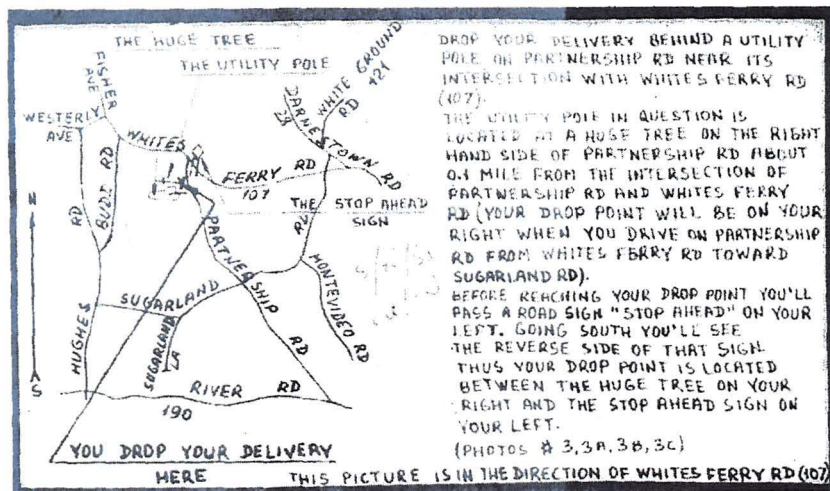
(U) Walker became Walkers, with Whitworth thrown in. It was not just a spy – it was an entire ring. Walker, a comm center operator and crypto technician when he had been in the Navy, had been supplying crypto key to the Soviets since 1968. Walker had recruited Jerry Whitworth, another Navy man in the same line of work, and when John Walker retired from the Navy in 1976, Whitworth continued to provide crypto material to Walker, who passed it on to the Soviets. He had recruited his brother, Arthur, and his son, Michael, and when arrested, John Walker was attempting to pass documents stolen from the Navy by Michael. The Walker ring had passed operational and technical documents to the Soviets. But more important, they had supplied crypto key for the KW-7, as well as several other devices, including the KW-37, KL-47, and KG-13.[47]

(U) The Walker operation was built around supplying used KW-7 key. Once a key had expired, the crypto security person (i.e., Walker) had seventy-two hours to destroy it. Walker (or Whitworth as the case may be) simply copied the key cards before destroying. Periodically (generally a matter of months), Walker would give the copied key cards to a Soviet agent using the dead drop procedure.

25X1

But in January of 1968, the same month that Walker first contacted the Soviets, the North Koreans captured the *Pueblo*, with a working KW-7 aboard. Though there is no direct evidence, there is ample indirect evidence that the KW-7 was sent to a research center south of Moscow, where it was presumably employed to read the taped messages once the Walker-supplied keys reached the Soviet Union. It was hardly a real-time operation, but from a long-term standpoint it was almost certainly the most lucrative espionage operation the Soviets ever had.[48]

(S) The Soviet operation of the Walker ring was a textbook in how to handle an espionage ring. They assigned only their very best KGB agents to the case. These agents went to unprecedented lengths to keep the operation from exposure, and the instructions that Walker received to dead drop operations were breathtakingly detailed and precise. The FBI believed that at any given time, only three people in the Soviet embassy in Washington were cleared for the operation. In Moscow, only the agents supervising the operation and a few top KGB officials were in on the secret.[49]

25X1

25X1

An expert witness testified at Jerry Whitworth's trial that "the damage thus done [by the Walker ring] could significantly, if not irrevocably, tilt the very strategic balance on which our survival as a nation depends." [50]

(S) NSG units used different keys, and since no one in the Walker ring was SI-cleared, it was unlikely that any cryptologic communications were being read. However, the Soviets did get information on other intelligence operations. The Navy's SOSUS array, used to track Soviet submarines, was probably compromised. 25X1

25X1

25X1

And finally, after frequent denials, Walker admitted providing key for tactical voice systems such as Nestor (KY-8/28/38), used in the Vietnam theater. Almost anything could have been passed on these nets, but they were used, for the most part, for operational information. [51]

(S) Processing the take that was potentially available would have strained the resources of the best espionage organization. Vitaly Yurchenko claimed that the KGB had "thousands" of people exploiting the material, and decrypted over a million messages, but this has never been confirmed. In 1994 a Russian HUMINT source who said he headed the exploitation effort claimed that his organization had only twenty-five people, and that daily production was low. He knew nothing of any other exploitation group. It is possible that only a fraction of the available material was exploited because of the inefficiencies inherent in the Soviet bureaucracy. [52]

(S) The Walker case brought a good many communications security deficiencies into sharp focus. Most basic was the lack of control of crypto keys, and the case resulted in a decision in 1988 to emphasize two-person control. It also brought about demands that electronic keying programs be accelerated. NSA became more insistent that the Navy reduce traffic volumes on individual nets, and quickened the pace of KW-7 modifications to surmount the crypto vulnerabilities that had been discovered earlier. NSA promised to accelerate the replacement of older crypto models with the new KG-84, which was capable of electronic keying. Meanwhile, the Navy broke up its nets into a four-ocean navy concept, and began 25X1

25X1

(U) These reforms were uncontroversial and relatively speedily accomplished. More divisive was the demand that the use of the polygraph be broadened. This reform was already being implemented within the military population at NSA when the Walker ring was exposed. But it undoubtedly reduced opposition to the polygraph in the wider armed services. NSA's Walter Deeley, the chief of Communications Security at NSA, informed the SSCI that he was reinstituting the crypto clearance, with its requirement for a non-lifestyle polygraph. His determination to force this despite doubt about his authority to do it on his own drew chuckles of admiration from the senators. [53]

(U) John Walker, the principal villain in the story, was paid over a million dollars by the Soviets. Jerry Whitworth received about $400,000, while the others received considerably lesser amounts. It is thus paradoxical that John Walker himself did not receive the longest prison sentence. In the days before his trial was to begin, he plea bargained to two concurrent life sentences plus ten years. Under the impenetrable mysteries of the federal sentencing guidelines, this means that he could theoretically get out of jail by age 75. His son pleaded guilty at the same time and received a twenty-five year sentence. Both agreed to cooperate with federal prosecutors.

(U) John Walker's cooperation was most unhelpful to his former friend and compatriot Jerry Whitworth. Whitworth, receiving decidedly bad advice from a coterie of San Francisco lawyers, chose to go to court. Walker testified at Whitworth's trial and was a key factor Whitworth's sentence of 365 years in prison and a $410,000 fine. Jerry Whitworth will die in prison.[54]

(U) POLLARD

(U) In September of 1979 the Navy hired a young Stanford graduate named Jonathan Jay Pollard to be an intelligence research specialist. Pollard was assigned to the Naval Intelligence Support Center (NISC) in Suitland, Maryland, where he was given a set of special clearances that would permit him to go to work. Included was access to SIGINT material.[55]
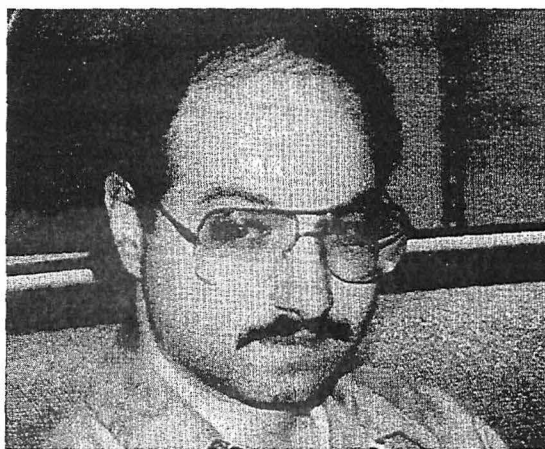
(U) In 1984 Pollard made contact with Israeli intelligence. He showed them samples of what he could provide, and they were

(U) Jonathan Pollard

interested. A flurry of meetings ensued, including trips to Paris and Israel. One of his contacts was Rafael Eitan, a legendary Mossad agent who had masterminded the capture of Adolf Eichmann and had headed the vengeance squad that tracked down and killed Palestinians who had participated in the 1972 Munich Olympics affair. Clearly, Pollard was regarded as a potential star in the espionage world.[56]

(U) Pollard was assigned to the antiterrorism alert center at NISC. His routine duties would thus give him access to information that Israel was interested in. But Pollard didn't stop at passive collection. He took a "shopping list" of desired information from his handlers and scanned DIA's computer databases for "hits." When he found something that

looked interesting, he simply asked the relevant office for the document. He was rarely refused.

(U) He accumulated documents quickly, and three times a week he put them into a briefcase and, using his courier pass, simply walked out with them. He batched the documents and once a week delivered them to a handler in a safe house in downtown Washington, D.C., not far from where Ronald Pelton lived. (They lived so close, in fact, that Pelton's girl friend noted surveillance, but decided that it was unrelated. It was FBI surveillance of Pollard.) There, the accountable documents would be copied so that Pollard could return the original; the rest they would not bother to copy. Once a month, Pollard made contact with his main handler, Joseph Yagur, who would evaluate the month's take and pay Pollard.[57]

(U) In September of 1985, Pollard's commanding officer at NISC, Commander Jerry Agee, learned that Pollard's computer searches had included excursions into some material unrelated to his job. Agee directed that a close watch be placed on Pollard. On October 25, a coworker reported to Agee that Pollard had apparently walked out of the building with classified documents. Surveillance of his activities became intense. A computer check showed that Pollard had acquired a huge number of documents on the Middle East, and a surreptitious search of his work spaces turned up none of them. At this point Agee called in Naval Investigative Service and the FBI.

(U) The net closed on Monday, November 18. Pollard was arrested trying to leave NISC in his Mustang with a satchel full of classified documents. Interrogation continued off and on all week, as Pollard gradually admitted more and more facts about his espionage. On Thursday he tried to flee to the Israeli embassy but was refused admittance. The FBI finally arrested him outside the embassy. Pollard and his wife Anne, who was deeply involved in the espionage, were out of options. His handlers had fled the country, and Israel was disowning him. Naval and FBI agents had recovered large numbers of documents in his apartment. A full confession was in order.[58]

(U) The Pollard arrest on November 21 came only three days before the arrest of Pelton and overlapped the exposure of the Walker ring. It heightened the sense of betrayal during the "Year of the Spy."

(TS//SI-UMBRA) NSA found that most of the documents that Pollard turned over to Israel were SIGINT. His handlers seemed to place high value in this source, and he exposed to Israel much of what NSA was doing on Middle East targets. He gave them information

25X1

(S//SI) Mostly, though, the damage related to NSA's overall capabilities. The Israelis

25X1
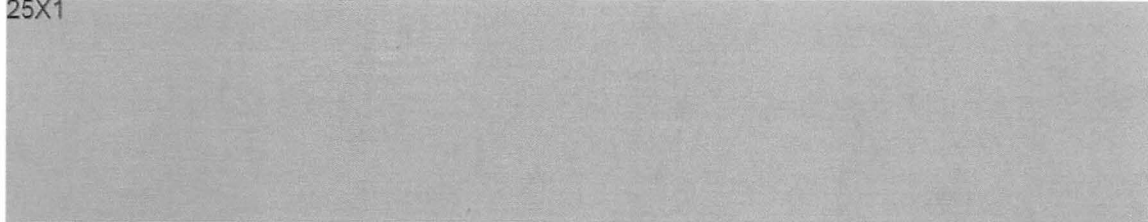
(U) The Department of Justice legal team wanted to try Pollard, but State pleaded that the diplomatic embarrassment would be too great. Ultimately DOJ fashioned a plea bargain that worked. Jay Pollard pleaded guilty and was sentenced to life in prison. (But the terms of a life sentence have already allowed him to petition for parole, which has been denied.) In return, Anne Pollard was given only two concurrent five-year terms and is already out of jail. All along the Pollards maintained that their motivation was ideology. But they received $2,500 in cash monthly, had $30,000 per year going into a "retirement account," and were treated to lavish all-expense paid trips to Europe and flashy jewelry by their Israeli handlers. NSA counterintelligence people who got acquainted with Pollard through interrogation regarded him as venal and devious. In his plea bargain he and his wife agreed to cooperate with the government, but their true cooperation has always been suspect.[61]

(U) HALL

(S//SI) James Hall, a young Army enlisted man, was assigned to INSCOM's Berlin site in 1983. Hall liked money, and in 1983 he contacted Soviet intelligence in Berlin. By this time he had become the Army's multichannel collection expert in Berlin, and he offered to share with the Soviets everything that he knew about the site and its mission. From February of 1983 to his reassignment to the U.S. in 1985, Hall did just that, in thirteen face-to-face meetings with his Soviet handlers, along with dead drops in various locations around Berlin.

(U) Prior to his reassignment, Hall had contacted an East German intelligence agent, Hussein Yildirim, who headed the post auto shop. In order to supplement his already substantial income, Hall agreed to provide East Germany the same information that he has giving the Soviets.

(U) During his year in the States, Hall continued to provide information to Yildirim, although the value was down because he was no longer associated with INSCOM. The Soviets also set up procedures for receiving Hall's information, but they were complex and difficult, and Hall chose to drop the association. Then, just a year later, he was back in Germany with 5th Corps and renewed his contacts with East Bloc intelligence. When he PCSed to Fort Stewart, Georgia, in 1988, he maintained contact with Yildirim, who moved to Florida to continue to work his contact with Hall. But by then the rigidities of the Cold

War were beginning to crack, and an East German source identified Hall as one of their agents.

(U) The FBI got Hall on a sting, in which one of their employees posed as a Soviet agent wanting to know what Hall had been providing to the East Germans. In a videotaped meeting Hall essentially confessed to espionage. He was arrested and is serving a forty-year sentence at Fort Leavenworth. Yildirim, arrested the day after Hall, is serving life without parole.[62]

(U//FOUO) Hall provided the Soviets and East Germans with "tradecraft" information. For instance, he gave them the entire National SIGINT Requirements List, amounting to a comprehensive targeting manual for the SIGINT system. He provided fifty USSIDs on various aspects of operations and manuals describing the entire SIGINT system and how it functioned. In return, Hall took away somewhere between $200,000 and $400,000. He was definitely in it for the money.

(U) CARNEY

(U) In the spring of 1990, an East German source reported to the CIA that he had information on a penetration of NSA. It was an old lead; the spy had been active in the mid-1980s, but was no longer in the business. Still, it could be another Pelton case, and NSA's counterintelligence branch went after the lead. The information was fragmentary and conflicting, and it became bogged down. Then a second source identified the spy as one "Yens Carney." The FBI traced Yens Carney to one Jeffrey Martin Carney, a former Air Force German linguist then living in the Soviet sector of East Berlin.

(S) Carney came from a difficult family background. He had dropped out of high school and had enlisted in the Air Force at seventeen. But he was extremely bright, and had been sent to German school, where he had gotten awards as the best German linguist in his class. From there he was sent to the ESC collection site at Marienfelde, West Germany in 1982. But he was in trouble almost immediately for missing a reporting situation in intercepted traffic, and he was decertified as a linguist. This began a downward spiral in his Air Force work relationship. Carney became argumentative and difficult on the job. He also realized that he was homosexual, which led to an identity crisis. In the midst of this turmoil, the immature Carney, then only nineteen, made a sudden decision to defect to East Germany, and went to Checkpoint Charlie, where he made contact with the other side. They, however, convinced him to spy, and he remained on the job.

(U) Carney began carrying a hidden camera in a Lipton Tea can. He collected miscellaneous documents while on burn detail and smuggled them out of the operations building. He met with his East German handlers every three weeks. In 1985 he PCSed to Goodfellow Air Force Base, where he continued to photograph documents. These he passed to his handlers during meetings in Berlin, Rio and Mexico City. But he became increasingly unstable and finally got his clearance pulled after an incident of uncontrolled

rage with his supervisors. At that point Carney defected to East Germany through Mexico City and Cuba (the same route that Martin and Mitchell had taken in 1961).

(U) He became a driver on the U-Bahn (Berlin's subway system) while continuing to work for East German intelligence. But he was in the wrong country. After the fall of the Berlin Wall it was not impossible to arrest spies, and Carney was arrested in April of 1991 outside his apartment. Brought back to the U.S. to stand espionage charges, he plea bargained for a twenty-five year sentence in exchange for his cooperation. He was debriefed, and NSA got a good picture of the damage. Fortunately, it was much less than it would have been had Carney worked within NSA.[63]

(U) Hall and Carney were bookend spies. They were both active in Berlin at the same time, one working in ASA, the other in ESC. They also worked for East German intelligence, although Hall passed information to the Soviets, too. Although neither had high-level information, between the two of them there was nothing the East Bloc did not know about U.S. SIGINT in Berlin.

(U) THE PUZZLE PALACE

(U) The 1982 publication of a book about NSA, *The Puzzle Palace*, by James Bamford, brought a new focus to the efforts of journalists and independent writers to break down the Agency's vaunted anonymity. *The Puzzle Palace* became the most significant breach in NSA's anonymity since David Kahn's *The Codebreakers* in 1967.

(U) As a former NSG enlisted man, Bamford had participated directly in the cryptologic process. While still in the Navy he had volunteered to help the Church Committee during its 1975 investigations. The late 1970s found him out of the Navy and working in Boston as a part-time private detective. He had gone to law school, but had not taken (or had not passed) the bar exam. In 1979 he approached publisher Houghton-Mifflin with a proposal to do a book on NSA. The publisher accepted and gave him a $7,500 advance.[64]

(U) Bamford proposed a comprehensive description and history of the Agency, a task that had never been attempted. Public Law 86-36 had served as a useful barrier against this type of research, but Bamford proved to be cleverer than others. He began with a barrage of requests for information under the Freedom of Information Act (FOIA). Through this and a lot of poking through publicly available information, he accumulated a small but useful stack of documents. Then he hit the Mother Lode – a collection of documents that William Friedman had deposited at the George Marshall Library at Virginia Military Institute in Lexington, Virginia. Among the scattered remains of Friedman's lifetime accumulations were copies of the *NSA Newsletter*, addressed to "NSA Employees and their families." Bamford then submitted a FOIA for the entire collection, using as his rationale the offending phrase indicating that the information had been intended for dissemination to uncleared people. NSA succeeded in redacting portions

using PL 86-36, but a disgruntled former NSA employee gave Bamford an almost complete collection which permitted him to fill in the redacted blanks.[65]

(U//FOUO) During the Church Committee hearings of 1975, the attorney general had asked his staff to investigate the legal culpability of the various intelligence agencies. Bamford FOIA'ed the resulting document, and he got most of it from the Justice Department. (Justice did not inform NSA because, they reasoned, the investigation was still on-going, and they could not inform a possible target of the investigation.) The document, with some Justice redactions, contained a good deal of information about the NSA-GCHQ relationship, and served as the basis for Bamford's information on Second Party issues. During the ensuing negotiations between NSA and Bamford's lawyer, the government claimed that the documents had been improperly released and should be returned under threat of prosecution. The lawyer, veteran civil rights attorney Mark Lynch, invited Justice to do just that, but no case was ever brought.[66]

(U//FOUO) Bamford knew how to get information. He drove through the NSA parking lot jotting down diplomatic license plates and checking known lists to see which countries maintained representatives at Fort Meade. He badgered retired NSA senior officials, including famed cryptanalyst Frank Raven, former head of NSA research and development Ray Tate, and former director Marshall Carter, for information, using as a wedge the information that he had already gotten from unclassified sources. Some pushed him aside, but others agreed to talk at length about NSA operations. Carter, for instance, talked with him for a day and a half at his retirement residence in Colorado Springs. All was technically unclassified, but it helped Bamford complete his mosaic. NSA policy makers felt that Raven was especially indiscreet, and lawyers indicated that it might be possible to prosecute, an eventuality that was interrupted by Raven's death.[67]

(U//FOUO) James Bamford broke new ground in intelligence agency research, and his techniques were adopted by others seeking to investigate reclusive federal agencies. He did it all within the limits of the law – through attributable interviews, FOIA'ed documents, and meticulous research in public libraries and newspapers, not with classified documents provided by unnamed accomplices under cover of darkness. He "wrote the book" on how to put together a comprehensive picture of an organization that wanted no such comprehensive picture. NSA's bottom-line assessment was that the individual pieces of the puzzle were – with one important exception – unclassified. Unfortunately for NSA, the entire mosaic turned out to be Top Secret Codeword.[68]

(U//FOUO) The single exception was the exposure of the relationship with the British. This was properly classified, and GCHQ was not amused.[69] Bamford's lawyers turned out to be tough and determined, and the information stayed in the public domain. The release of classified material by, of all organizations, the U.S. Justice Department, left NSA non-plussed.

(U) Bamford produced a book that was deeply flawed by mistaken analyses of collected data. It contained much misinformation, an exaggerated view of NSA's capabilities, and a preoccupation with a lack of statutory controls on NSA. Like Jack Anderson's columns,

the book – in the opinion of many NSA leaders – did grave damage to national security while maintaining the guise of legal methodology.

(U) THE AMERICAN LIBRARY ASSOCIATION SUIT

(U) Following publication of *The Puzzle Palace*, General Faurer sent NSA's Meyer Levin to the Marshall Library to see where Bamford had gotten so much of his information. Levin discovered that an archivist had given Bamford access to sequestered portions of the Friedman collection. NSA re-sequestered the documents, and was challenged in court by Bamford's lawyer, Mark Lynch of the American Civil Liberties Union, acting on behalf of the American Library Association.[70]

(U) This time the law was on NSA's side. Since the early negotiations with Lynch over the FOIA'ed Justice Department records, President Reagan had signed a new executive order, 12033, which permitted publicly available documents to be withdrawn if it could be shown that they had been improperly declassified. NSA's argument was supported by the U.S. District Court of Appeals in 1987, which dismissed the case against NSA and ruled that the plaintiff, the American Library Association, lacked standing.[71]

(U) EPILOGUE

(U) On November 9, 1989, the East German government announced that its citizens could leave the country without special permission. Within hours, jubilant crowds were surging through the formerly impenetrable Berlin Wall, to be greeted by their West German countrymen. The crowds sang and danced that night. They hacked at chunks of the infamous Wall, and swirled through the Brandenburg Gate. It was liberation day.

(U) November 9 was the culmination of both long- and short-term events. Such imponderables as the inherent weaknesses of Marxism and the latent inefficiencies of the Soviet state moved glacially, but they eventually produced Gorbachev, a man who recognized the situation and tried to reform it. *Glasnost* and *perestroika* (openness and economic restructuring) were the pillars of his reform program.

(U) But short-term events overtook socialist reform. It was not necessary for the Soviet government to invent a new form of socialism – a dandy economic model glittered just across the Iron Curtain in Western Europe. Encouraged to devise their own socialist economic models, Hungary and Poland moved quickly. In East Germany, Eric Honecker, the long-time Communist Party boss, thumbed his nose at reform, and got in return unrest and agitation. Agitation turned into street demonstrations in August. Gorbachev withdrew Soviet support for more repression, and without this guarantee the East German authorities could no longer contain the population. In October, Gorbachev personally told Honecker that the Soviet forces in his country would not come to his rescue. Honecker, sick with gall bladder cancer, knew the end was near.

(U) So the end of the Cold War swept in like a sudden storm, leaving prognosticators dazed. It happened so fast and went so far that it would take a breathless world some considerable time to assess the event.

(U) For the cryptologic community, it was a new beginning. Nothing like it had happened since the end of World War II. Major target countries disappeared literally overnight. Foreign relationships changed, and former enemies became new Third Parties with scarcely an intervening day.

(U) But from a historical perspective, it was also an ending, a milepost in the course of history. The bipolar world had defined American cryptology for forty-four years. It was now over, and it was time to write the history.

(U) Notes

1. (U) Interview, David Boak, by Tom Johnson, 20 January 1998.

2. (U) Deputy Director's files, 96026, Box 14, Schlesinger papers, NSA memo 21 October 1966.

3. (U) Dick Nelson and Julie Koenen-Grant, "A Case of Bureaucracy in Action: the U.S. Embassy in Moscow," *International Journal of Intelligence and Counterintelligence* (Fall, 1993).

4. (U) Inman interview. Interview, John Wobensmith, by Tom Johnson, 8 November 1996, OH 34-96, NSA. de Graffenreid interview.

5. (U) It appears that PL 86-36/ approached Faurer rather than his counterpart, William Casey, based on a close professional relationship in the area of cryptologic cooperation that they had established after Faurer had become DIRNSA. See interview, Lt. Gen. Lincoln D. Faurer, by Tom Johnson, 20 August 1998, OH 15-98, NSA; CCH Series XII.D., "Gunman," Evaluation of Project Gunman by S65, 28 January 1985. Wobensmith interview. Interview, Stephen B. Carter, by Tom Johnson and Benjamin Hoover, 20 July 1998, OH 14-98, NSA. Deputy Director's files, 96026, Box 14, Schlesinger papers.

6. (U) Carter interview. CCH Series XII.D., "Gunman."

7. (U) Interview, PL 86-36/50 by Tom Johnson, 4 August 1998, OH 15-98, NSA. Wobensmith interview. Carter interview. CCH Series XII.D., "Gunman." Deputy Director's files, 96026, Box 14, "CIA Damage Assessment."

8. (U) XII.D., "Gunman." Deputy Director's files, 96026, Box 14, "CIA Damage Assessment."

9. (U) Deputy Director's Files, 96026, Box 14, "CIA Damage Assessment;" Box 10, "Moscow Embassy - 1987."

10. (U) Faurer interview; Wobensmith interview.

11. (U) Deputy Director's files, 96026, Box 14, Schlesinger paper; "Lonetree-Bracy Chronology and Damage Assessment."

12. (U) Nelson and Koenen-Grant, "A Case of Bureaucracy in Action...." Deputy Director's files, 96026, Box 10, "Moscow Embassy - 1987"; "Laird Panel."

13. (U) Reagan Library, NSF, in CCH Series XIV.J, "Embassy Security." Deputy Director's files, 96026, Box 10, "Moscow Embassy - 1987."

14. (U) Michael Beschloss and Strobe Talbot, *At the Highest Levels: The Inside Story of the End of the Cold War* (Boston: Little, Brown and Company, 1991), 33-34, 94.

15. (U) Polmar and Allen, *Merchants of Treason*, 181.

16. (U) Deputy Director's files, 96026, Box 14, "Prime Case Damage Assessment."

17. (U) Ibid.

18. (U) Deputy Director's files, 96026, Box 9, "Milkman Damage Assessment." 5001, 40. Polmar and Allen, *Merchants of Treason*, 40.

19. (U) Deputy Director's files, 96026, Box 9, "Milkman Damage Assessment."

20. (U) Norman Polmar and Thomas B. Allen, *Merchants of Treason* (New York: Delacourte Press, 1988), 205-06.

21. (U) Deputy Director's files, 96026, Box 4, "Pelton File."

22. (U) NSA, S4 videotape briefing on Pelton. Deputy Director's files, 96026, Box 14, "Pelton Damage Assessment."

23. (U) NSA, GC office files, U.S. v. Pelton working papers. Deputy Director's files, 96026, Box 14, "Pelton Damage Assessment."

24. (U) NSA, S4 videotape briefing on Pelton. NSA, GC office files, U.S. v. Pelton, Pleadings.

25. (U) Ibid.

26. (U) S4 Pelton videotape. PL 86-36/50 interview.

27. (U) Polmar and Allen, *Merchants of Treason*, 207-14. Interview, PL 86-36/50 by Tom Johnson, 20 February 1997, OH 5-97, NSA.

28. (U) PL 86 36/5 interview.

29. (U) Deputy Director's files, 96026, Box 4, "Pelton File."

30. (U) Ibid. PL 86 36/5 interview.

31. (U) PL 86 36/50 interview.

32. (U) Interview, William P. Crowell, by David A. Hatch and PL 86-36/50 29 May 1996, OH 16-96, NSA. PL 86 36/50 interview. NSA, GC office files, Pelton file. PL 86-36/50 interview.

33. (U) PL 86-36/5 interview.

34. (U) Ibid.

35. (U) NSA, GC office files, U.S. v. Pelton, working papers. Deputy Director's files, 96026, Box 14, "Pelton Damage Assessment"; "CIA Damage Assessment." Ch A2 files, 96228, Box 4, A/J Joint Conference 1987; Box 6 "T230."

36. (U) Ch, A2 files, 96228, Box 4, "Miscellaneous Studies."

37. (U) NSA, GC office files, Pelton; U.S. v. Pelton, Working Papers. Interview, Lt. Gen. William Odom, by Tom Johnson, 19 August 1997, OH 13-97, NSA.

38. (U) NSA, GC office files, "U.S. v. Pelton, Working Papers." Bradlee quote is from *Time*, June 2, 1986.

39. (U) NSA, GC office files, Pelton. Odom interview.

40. (U) NSA, GC office files, Pelton.

41. (U) Ibid., Durenberger letter to SSCI members, 7 May 1986.

42. (U) Interview, PL 86-36/50 USC by Charles Baker and Tom Johnson, 2 February 1993, OH 2-93, NSA. Boak interview. U.S. Department of Justice, Federal Bureau of Investigation, "John A. Walker Espionage Network," July 1987.

43. (U) Telephone interview with Joseph Maguire, by Tom Johnson, 19 December 1997. Tate interview. Rosenblum interview.

44. (U) Ibid.

45. (U) FBI, "John A. Walker Espionage Network." Carter interview.

46. (U) Deputy Director's files, 96026, Box 14, "CIA Damage Assessment." Pete Early, *Family of Spies: Inside the John Walker Spy Ring* (New York: Bantam Books, 1988). FBI, "John A. Walker Espionage Ring."

47. (U) Early, *Family of Spies*. NSA Archives, acc nr 20960, CBOF 33.

48. (U) Newton, *The Capture of the USS Pueblo...*, 157-59. Polmar and Allen, *Merchants of Treason*, 18.

49. (U) FBI, "John A. Walker Espionage Ring."

50. (U) Deputy Director's files, 96026, Box 1, "Overview of Damage from Recent Espionage." NSA Archives, acc nr 20960, CBOF 33. FBI, "John A. Walker Espionage Ring."

51. (U) Deputy Director's files, 96026, Box 14, "CIA Damage Assessment."

52. (U) FBI, "John A. Walker Espionage Ring." Interview, Michael Jacobs, by Tom Johnson and Ben Hoover, 22 June 1998, OH 11-98, NSA.

53. (U) NSA Archives, acc nr 20960, CBOF 33; acc nr 19217, H03-0102-6. Deputy Director's files, 96026, Box 14, "CIA Damage Assessment."

54. (U) FBI, "John A. Walker Espionage Ring."

55. (U) Polmar and Allen, *Merchants of Treason*, 292-87.

56. (U) Ibid., 295.

57. (U) Ibid., 288-90.

58. (U) Ibid., 291-93.

59. (U) PL 86-36/50 interview. CCH Series XII.D., Pollard file, debriefing notes, 13/14 August 1986.

60. (U) Ibid.

61. (U) Polmar and Allen, *Merchants of Treason*, 288-89, 297.

62. (U) S4 files, James Hall, 63.

63. (U) S4 files, Jeffrey Carney.

64. (U) Interview, Meyer J. Levin, by Robert Farley and Tom Johnson, 14 January 1987, OH 2-87, NSA. Paul Constance, "How Jim Bamford Probed the NSA," *Cryptologia*, 21 (January 1997), 71-74.

65. (U) David C. Martin, "Putting Secret Puzzles Together," *The Washingtonian* (March 1983), 89-95. Constance, "How Jim Bamford Probed the NSA," 72. Levin interview.

66. (U) Levin interview. Constance, "How Jim Bamford Probed the NSA."

67. (U) Levin interview. Interview, LTG Marshall S. Carter, by Robert Farley, 3-6 October 1988, OH 15-88, NSA.

68. (U) NSA, CCH Series VI.G.4.

69. (U) Ibid.

70. (U) Levin interview. NSA, CCH Series VI.G.2.1.

71. (U) Ibid.

(U) Glossary

ABM – antiballistic missile

ACE – American Council on Education

ACRP – Airborne Communications Reconnaissance Program

ACSI – Assistant Chief of Staff, Intelligence (Army)

ADC – Assistant Director for COMSEC

AFSC – Armed Forces Security Center (Thai military organization)

AFSCC – Air Force Special Communications Center

AFSS – Air Force Security Service

AFTAC – Air Force Technical Applications Center

ALP – Australian Labor Party

ALTROF – alternate remote operations facility

AMPS – Automated Message Processing System

ANO – Abu Nidal Organization

ANZUS – Australia, New Zealand and the United States (diplomatic treaty)

ARDF – airborne radio direction finding

AROF – A Remote Operations Facility

ARVN – Army of the Republic of Vietnam (i.e., South Vietnam)

ASA – Army Security Agency

ASRP – Airborne SIGINT Reconnaissance Platform

ASTW – Agency Standard Terminal Workstation

ASW – antisubmarine warfare

AT&T – American Telephone and Telegraph Corporation

BND – Bundes Nachrichten Dienst PL 86-36/50 USC 3605

BROF – B Remote Operations Facility

BSU – Bauded Signals Upgrade

BWI – Baltimore-Washington International Airport

C3CM – command, control and communications countermeasures

CBR – chemical, biological and radiological

CCP – Consolidated Cryptologic Program

CDAA – circularly disposed antenna array

CDC – Control Data Corporation

CENTCOM – Central Command

25X1, 6

CINCPAC – Command-in-Chief, Pacific

CNO – Chief of Naval Operations

COC – Collection Operations Center

COINS – Community On-line Information System

CONUS – continental United States

COPES – Collection Operations Position Evaluation Standard

COS – Chief of Station (CIA)

CSG – cryptologic support group

CSOC – Current SIGINT Operations Center

CSS – Central Security Service

DARPA – Defense Advanced Research Projects Agency

DAO – Defense Attaché Office

DCA – Defense Communications Agency

DCI – Director of Central Intelligence

DDF – Deputy Director for Field Management and Evaulation

DDO – Deputy Director for Operations (NSA)

DDR – Deputy Director for Research

DDT – Deputy Director for Telecommunications and Computer Services

DEA – Drug Enforcement Administration

DEFCON – Defense Condition

DEFSMAC – Defense Special Missile and Astronautics Center

DES – data encryption standard

DGTS – Directorate General of Technical Security (South Vietnamese SIGINT service)

DIRNSA – Director, NSA

DO – Director for Operations (CIA)

DOJ – Department of Justice

DMZ – demilitarized zone

DSA – Defense Supply Agency (U.S. DoD) or Defense Security Agency (South Korea)

DSD – Defence Signals Directorate

DSCS – DoD Satellite Communications System

DSE – direct support element (Navy)

DSSCS – Defense Special Security Communications System

GDRS – General Directorate of Rear Services (North Vietnamese logistics network) supporting infiltration into South Vietnam)

DSU – direct support unit (Army)

ECCM – electronic counter-countermeasures

ECM – electronic countermeasures

ESC – Electronic Security Command

ESM – electronic (warfare) support measures

EUCOM – European Command

EW – electronic warfare

FANX – Friendship Annex

FCC – Federal Communications Commission

FISA – Foreign Intelligence Surveillance Act

FOIA – Freedom of Information Act

FRG – Federal Republic of Germany

FSCS – Future SIGINT Capabilities Study

GE – General Electric Company

25X1, 6

GROF – G Remote Operations Facility

GSA – General Services Administration

GSFG – Group of Soviet Forces Germany

GTOF – G Tennis Operations Facility

HAC – House Appropriations Committee

HPSCI – House Permanent Select Committee on Intelligence

IATS – Improved AG-22 Terminal System

IC – intelligence community

ICBM – intercontinental ballistic missile

IDA/CRD – Institute for Defense Analyses/Communications Research Division

IDDF – Internal Data Distribution Facility

IEEE – Institute of Electrical and Electronics Engineers

IFF – identification friend or foe

ILC – international commercial

INR – [Bureau of] Intelligence and Research (State Department)

INSCOM – Intelligence and Security Command

IR – infrared

IRBM – intermediate range ballistic missile

ITAR – International Traffic in Arms Regulation

ITT – International Telephone and Telegraph [corporation]

I&W – indications and warning

JASDF – Japanese Air Self-Defense Force

JOPS – J Operations Processing System

JUSMAG – Joint U.S. Military Assistance Group

KAL – Korean Air Lines

KC – Khmer Rouge (communist insurgent force in Cambodia)

LLVI – low-level voice intercept

LMSC – Lockheed Missile and Space Corporation

LPG – London Processing Group

MAAG – Military Advisory Assistance Group

MAC – Military Airlift Command

MACV – Military Assistance Command Vietnam

MCSF – Mobile Cryptologic Support Facility

MEAR – Maintenance, Engineering, and Architecture (team)

MENAS – Middle East and North Africa Summary

MIJI – meaconing, intrusion, jamming and interference

MO – method of operation

MIRV – multiple independently targetted re-entry vehicle

MODE – Monitoring of Overseas Direct Employment

NBS – National Bureau of Standards

NCC – National Cryptologic Command

NCO – noncommissioned officer

PL 86-36/50 USC 3604

NIO – National Intelligence Officer

NISC – Naval Intelligence Support Center

NIST – National Institute for Standards and Technology

NNBIS – National Narcotics Border Interdiction System

NOB – new office building (American embassy chancery, Moscow)

NOIWON – National Operations and Intelligence Watch Officers Network

NORAD – North American Air Defense Command

NPIC – National Photographic Interpretation Center

NRL – Naval Research Laboratory

NRO – National Reconnaissance Office

NSASAB – NSA Scientific Advisory Board

NSC – National Security Council

NSCID – National Security Council Intelligence Directive

NSF – National Science Foundation

NSG – Naval Security Group

NSOC – National SIGINT Operations Center

NTIA – National Telecommunications and Information Administration

NTISSC – National Telecommunications Information Security Committee

NVA – North Vietnamese Army

OCMC – Overhead Collection Management Center

OCR – optical character reader

OMB – Office of Manpower and Budget

ONI – Office of Naval Intelligence

ONR – Office of Naval Research

OPEC – Organization of Petroleum Exporting Countries

OSD – Office of the Secretary of Defense

OSHA – Occupational Safety and Health Administration

OTAR – over-the-air rekeying

PACAF – Pacific Air Forces

PACOM – Pacific Command

PARPRO – Peacetime Aerial Reconnaissance Program

PC – Problem Center

PDF – Panamanian Defense Force

PERSUM – NSA personnel summary

PFIAB – President's Foreign Intelligence Advisory Board

PFLP – Popular Front for the Liberation of Palestine

PLO – Palestine Liberation Organization

PRC – People's Republic of China

PX – post exchange facility

RASIN – Radio Signal Notation

RCA – Radio Corporation of America

PL 86-36/50 USC 3604

RIF – reduction in force

ROC – Republic of China (Taiwan)

ROF – remote operations facility

ROFA – Remote Operations Facility

RSA – Rivest, Shamir and Adelman [name of an encryption algorithm]

SAC – Strategic Air Command

SACEUR – Supreme Allied Commander Europe

SAFSPD – Secretary of the Air Force Special Projects Division

SALT – Strategic Arms Limitation Talks

SCA – Service Cryptologic Agency

SCE – Service Cryptologic Element

PL 86-36/50 USC 3604

SDS – Students for a Democratic Society

SIGDASYS – SIGINT Inter-Connected Data System

SIGSUM – SIGINT Summary

SIOP – single integrated operational plan (U.S. nuclear targetting plan)

25X1, 6

SLO – SIGINT Liaison Office

SOO – Senior Operations Officer

SORS – SIGINT Overhead Reconnaissance Subcommittee

SOSUS – Sound Surveillance System

SOUTHCOM – Southern Command

SSA – Special Support Activity

SSBN – ship submersible, nuclear

SSCI – Senate Select Committee on Intelligence

SSO – Special Security Office

STU – Secure Telephone Unit

SUA – Shan United Army

SUSLO – Senior U.S. Liaison Officer [to GCHQ]

TACREP – tactical SIGINT report

TAREX – Target Exploitation

TCOF – Transient Collection Operations Facility

TDOA – time difference of arrival

TENCAP – Tactical Exploitation of National Capabilities

25X1, 6

TVD – Soviet term for theater of military operations (TMO)

UKUSA – United Kingdom-United States [agreement on cryptologic matters]

USAFE – U.S. Air Forces Europe

USAFSS – U.S. Air Force Security Service

USIB – United States Intelligence Board

U&S – unified and specified [commanders/commands]

USSAG – United States Support Activities Group (the successor to MACV)

USSID – U.S. Signals Intelligence Directive

VTA – Soviet military air transport arm

ZI – Zone of the interior (i.e., continental United States)

(U) Sources

(S//SI) The time period covered by Books III and IV is so recent that there were few secondary histories of any of it. Notable exceptions were Robert Newton's very fine history of SIGINT and the Falklands Crisis, and PL 86-36/50 Cryptologic Quarterly article on public cryptography during the Inman administration. Sharon Maneki's forthcoming history of SIGINT and the Panama Canal negotiations also played a useful part. There were few other internally published secondary sources available. Thus, Books III and IV were produced through research in primary documents. The two most extensive collections were:

1. (U) The NSA Archives. This consists of two categories of records:

   a. (U) Archived records, which have been accessioned into the permanently retained collection. These appear in footnotes as an accession number (e.g., acc nr 39471) and a shelf location (e.g., H03-0311-4).

   b. (U) Retired records. These are still the property of the donating office and have not been accessioned. They are identified by a shipment and box number, e.g., 43852, 105915-56.

2. (U) The historical collection of the Center for Cryptologic History (CCH), S542. This collection of historical documents actually predates the archived collection, and it contains records going back to the earliest days of cryptology. Records in this collection generally duplicate those in the Archives, but they are maintained as a separate file for ease of access by historians. The CCH collection is organized into the following series:

   I.   Pre-1915
   II.   1915-1918 (World War I)
   III.   1919-1939 (Interwar period)
   IV.   1939-1945 (World War II)
   V.   1946-1952 (pre-AFSA and AFSA period)
   VI.   1952-present
   VII.   Special and miscellaneous collections
   VIII. Crisis files
   IX.   Press and journal items
   X.   References
   XI.   Papers collected by NSA and pre-NSA officials
   XII.   Papers collected by NSA historians
   XIII. Equipment manuals
   XIV.   COMSEC documents
   XVI.   Cryptologic papers duplicated from presidential libraries

Citations from this collection are by series number, followed by subseries designations, for instance, VI.A.1.9.

3. (U) Oral histories. NSA's oral history collection now comprises nearly 600 interviews with mostly NSA officials on cryptologic topics. This collection is extremely useful, especially in view of the paucity of official records. Very few subjects covered by this history were done without reference to oral histories. They are identified by the year and a one-up number, e.g., 12-94. The most useful for Books III and IV were:

Lew Allen, Jr., 19-96

Eugene Becker, 11-96

Joseph M. Bellomo, 19-96

Edward Benz, 33-96

Frederick J. Berghoff, 50-94

Frederick Bergman, 1977, unnumbered

Richard L. Bernard, 15-94 and 18-96

H. Judd Berry, 9-86

PL 86-36/50 December 1996, unnumbered

David G. Boak, May 1998, unnumbered

Norman Boardman, 3-86

Bonsall, Sir Arthur W., 40-95

James V. Boone, 27-86 and unnumbered interview, June 1998

Paul Brady, 22-95

PL 86-36/50 USC 1976, unnumbered

Alan D. Cameron, Edward A. O'Connor and James A. Wright, 6-92

Richard L. Canova and Perry Iannaconi, 25-96

Stephen B. Carter, 13-98

Dennis Chapman, 2-97

George R. Cotter, 7-96

William P. Crowell, 16-96

PL 86-36/50 September 1997, unnumbered

Kenneth deGraffenreid, 5-98

John P. Devine, 1-95

PL 86-36/50 January 1997, unnumbered

PL 86-36/50 USC 14-86

James W. Dyer, Gerald F. Kozlowski, PL 86-36/50 USC 3604 and Robert F. Stahley, 4-93

Lincoln D. Faurer, 8-87

Thomas J. Fogarty, 1997, unnumbered

PL 86-36/50 USC 30-87

PL 86-36/50 USC 3604 15-96

Thomas L. Glenn, 4-86

PL 86-36/50 USC 3604 5-97

John R. Harney, 32-87

PL 86-36/50 USC 3604 July 1997, unnumbered

Robert J. Hermann, 45-94

PL 86-36/50 USC 3604 February 1997, unnumbered

James G. Hudec, 17-96

PL 86-36/50 USC 3604 6-86

Francis P. Hyland, 11-97

Bobby R. Inman, 9-97

Edward Jacobs, 4-97

PL 86-36/50 USC February 1997, unnumbered

PL 86-36/50 USC 3604 10-97

Edward Jacobs, 4-97

Michael Jacobs, 10-98

PL 86-36/50 USC 3604 13-86

William T. Kvetkas, 25-96

Meyer J. Levin, 2-87

PL 86-36/50 USC 3604 18-86

PL 86-36/50 10-87

PL 86-36/50 USC 3604 1-96

Doyle E. Larson, 15-94, 15-97

PL 86-36/50 1997, unnumbered

PL 86-36/50 USC 3604 8-92

Joseph Maguire, February 1997 and April 1998, unnumbered

PL 86-36/50 USC 3604 7-97

Sir Peter Marychurch, 11-89

PL 86-36/50 USC 3604 19-85

PL 86-36/50 USC 3604 January 1997, unnumbered

PL 86-36/50 USC 3604 2-93

PL 86-36/50 USC 23-94

PL 86-36/50 USC 3604 March 1997, unnumbered

Robert Morris, 41-94

Robert Mueller, 6-8

PL 86-36/50 USC January 1997, unnumbered

William E. Odom, 13-97

PL 86-36/50 34-96

PL 86-36/50 USC 3604 September 1997, unnumbered

Harold L. Parish, 20-82

Russel L. Parker, 52-94

Cecil J. Phillips, 23-93

Howard S. Pierce, 12-98.

PL 86-36/50 USC 3604 1966, unnumbered

Whitney E. Reed, 39-96

Robert E. Rich, 12-97

Elizabeth Rindskopf, 4-98

PL 86-36/50 USC 3604 January 1997, unnumbered

Howard E. Rosenblum, 3-91

PL 86-36/50 USC 3604 8-97
PL 86-36/50 USC 3604 15-97
PL 86-36/50 USC 3604 1-92

  Donald M. Showers, by Arthur D. Baker III, 1992.
PL 86-36/50 USC 14-97
PL 86-36/50 USC 3604 AIA oral history

  Kermit H. Speierman, 2-86

  John Spencer, 29-93

  Carl W. Stapleton, ESC interview, 1986
PL 86-36/50 USC 3604 24-86

  William O. Studeman, 5-91

  Raymond L. Tate, 35-96
PL 86-36/50 USC 3604 12-96

  David H. Williams, 23-87

  John Wobensmith, 34-96

  Richard Young and PL 86-36/50 USC 3604 1977, unnumbered

  Milton Zaslow, 17-93
PL 86-36/50 USC 3604 4-92

4. (U) Internally published, classified, histories included the following:

(U) Abbott, Walter D., Jr. "Establishment of the 25X6 1979," *Cryptologic Quarterly*, 12:5 (Noforn Issue, 1993)

(U) Boak, David G. A History of U.S. Communications Security [The David G. Boak Lectures]. Fort Meade: NSA, 1973.

(U) Bradburn, Maj Gen David D. (USAF, Ret.), Col John O. Copley (USAF, Ret.), Raymond B. Potts and Roger E. Thayer. *The SIGINT Reconnaissance Satellites*. Washington: NRO, 1994

(U PL 86-36/50 USC 3604 Interview. *Cryptolog*, December 1976.

(U) Campbell, Norman J. "Guardrail: A Joint Tactical SIGINT Support System," *Cryptologic Spectrum* (Spring 1975), 15-18.

(U PL 86-36/50 USC 3604 "Ethiopia, 1972-1975: An Inside View of Indications and Warning," *Cryptolog* (1st Issue, 1978), 1-8.

(S//SI PL 86-36/50 USC 3604 "The Dozier Kidnapping: A Story of Successful SIGINT Cooperation," *Cryptologic Quarterly*, 10:3-4 (Fall/Winter 1991), 1-29.

(U) Filby, Vera. *The Soviet Invasion of Afghanistan: A Cryptologic History*. U.S. Cryptologic History, Special Series, Crisis Collection, Vol. 8. Fort Meade: NSA, 1993.

(U) [PL 86-36/50 USC 3604] "The 1983 War Scare in U.S.-Soviet Relations, *Studies in Intelligence*, 39:4 (1995), 61-72.

(S//SI) [PL 86-36/50 USC 3604] "Radio Technical System for Short-Range Navigation (RSBN)," *Cryptologic Quarterly*, 16:1 (Spring 1997), 75-89.

(U) Hanyok, Robert J. "Scaling Down NSA," *NSA Newsletter*, January 1995.

(U) _____. "The Relevant Truths: SIGINT Issues of the Indochina War, 1950-1975 (Part II)" *Cryptologic Quarterly*, 16:3 (Fall 1997), 1-50.

(U) [CIA Statute] The Story of the Hughes Glomar Explorer," *Studies in Intelligence* (Fall 1978), 1-50.

(U) [PL 86-36/50 USC 3604] "OPSEC as a Management Tool." *Cryptolog* (1st issue, 1972), 7-9.

(U) [PL 86-36/50 USC 3604] *PURPLE DRAGON: The Origin and Development of the United States OPSEC Program.* U.S. Cryptologic History, Series VI, Vol. 2. Ft. Meade: NSA, 1993.

(U) [PL 86-36/50 USC 3604] *NSA's Involvement in U.S. Foreign SIGINT Relationships through 1993.* U.S. Cryptologic History, Series VI, Vol. 4. Ft. Meade: NSA, 1995.

(U) [PL 86-36/50 USC 3604] "NSA Comes Out of the Closet: The Debate Over Public Cryptography in the Inman Era." *Cryptologic Quarterly*, 15:1 (Spring 1996), 5-44.

(U) [PL 86-36/50 USC 3604] "The Platform Network Evolution," *Cryptologic Quarterly*, 9:4 (Winter 1991).

(U) Newton, Robert E. *The Falklands, 1982: An American Perspective.* U.S Cryptologic History Series, Special Series, Crisis Collection, Vol. 4. Ft. Meade: NSA, 1991.

(U) Nolte, William. *NSA Actions During the Iranian Hostage Crisis: An Interim History.* U.S. Cryptologic History Series, # 1. Ft. Meade: NSA, 1981.

(U) _____. *Project Tennis: A History of Satellite Remoting, 1968-1977.* Fort Meade: NSA, 1977.

(U) [PL 86-36/50 USC 3604] "Foreign SIGINT Operations: The Legal Side." *IAI International Notes and News*. Fort Meade: NSA, 1993.

(U) [PL 86-36/50 USC 3604] "The Great Conversation." *Cryptolog* (1st Issue 1992), 2-6.

(U) Stahley, Glenn F. *Fifty Years of Mathematical Cryptanalysis.* Fort Meade: NSA, 1988.

(U) Ware, Willis, et al. "Report of the Second Computer Study Group," *NSA Technical Journal* 19:1 (Winter 1974), 21-61.

(U) [Wiley, Edward] *On Watch: Profiles from the National Security Agency's Past 40 Years*. Ft. Meade: NSA, n.d.

(S//SI) PL 86-36/50 "The Tacksman Project: A SIGINT Success Story," *Studies in Intelligence* (Fall, 1991), 21-31. (Published by CIA.)

5. (U) Internal, but unpublished, historical studies often contain important information. The more important ones used in this study were:

(U) PL 86-36/50 USC 3604 "The Reemployed Annuitant (REA) Program in NSA: An Evaluation of the Agency Archives." CCH files.

(S//SI) PL 86-36/50 USC 3604 "A Historical Overview of the U.S. SIGINT Effort in Turkey," October 1988, in CCH Series VI.K.1.4.

(U) Filby, Vera. "A Decade of Change in SIGINT Reporting: The 1970s." 7 August 1979. CCH Series XII.D.

(U) Finnegan, Jack. "IOSS and After." 1987. Available at HQ INSCOM, Fort Belvoir, Virginia.

(U) PL 86-36/50 USC 3604 "Support to Military Operations: NSA's Contribution to Operation 'Just Cause'." NSA/PGIP Class 9101.

(U) "Historical Study of NSA Telecommunications, Annual, 1973-1975." CCH Series A.1.10.

(U) "History of the Poppy Satellite System." October 1978. CCH Series XII.OO.

(U) "History of Yakima Research Station: PL 86 36/50 CCH Series VI.I.1.3.

(S//SI) PL 86-36/50 USC 3604 History of 25X1 CCH Series VII.89.

(U) PL 86-36/50 USC 3604 "Development of the Australian SIGINT Organization: A Synopsis of Major Events from 1947 to 1992." CCH Series VI.J.1.2.1.

(U) PL 86-36/50 USC 3604 "A Brief History of GROF." CCH files, 1996.

(U) PL 86-36/50 USC 3604 Draft history of OTAR, 1998, in CCH Series XII.D.

(U) PL 86-36/50 USC 3604 "International Terrorism and the National Security Agency: The Evolution of a Centralized Response." 1986. CCH files.

(U) Millington, Henry. Untitled manuscript on the history of PL 86-36/ CCH collection.

(U) Moore, Elizabeth. "As We Were: An Informal History of Bad Aibling Station, 1936-1988." CCH Series VI.I.1.10.

(U) PL 86-36/50 USC 3604 "History of Menwith Hill Station." CCH Series VI.I.2.11.

(U PL 86-36/50 USC 3604 Jr. "The Eagle Watches the Bear: Soviet Involvement in Afghanistan, 1978-1980." CCH Series VIII.44.

(U) "SIGINT Support to Military Operations" [the Hermann Study]. NSA retired records, 28792, 80-079.

(U) "Summary of Statutes Which Relate Specifically to NSA and the Cryptologic Activities of the Government." Undated manuscript file in CCH files.

(U) PL 86-36/50 USC 3604 Draft history of computer security at NSA. CCH files.

6. (U) There are several important documents or collections of historically valuable documents that repose in various locations within NSA. The most useful were:

(U) PL 86-36/50 USC 3604 Study. 1978. CCH Series XII.D.

(S//SI) CDO 25X6 iles. NSA, Directorate of Foreign Relations.

(S//SI) CDO 25X6 files. NSA, Directorate of Foreign Relations.

(S//SI) CDO 25X6 files. NSA, Directorate of Foreign Relations.

(U) CDO UK files. NSA, Directorate of Foreign Relations.

(U) Drawstring Task Force Report, 10 December 1973. NSA Archives, acc nr 32545.

(U) Files of NSA's deputy directors, retired records, shipment nr 96026, boxes 104545-10458. This collection was the single most valuable source for these two books.

(U) Files of the chief, A2 (office of Soviet analysis), retired records, shipment nr 96226, boxes 105951-56.

(U) History of the Soviet Nuclear Weapons Program. PL 86-36/50 USC 3604 NSA. DCI/ICS 5321/87JX.

(U) HF Modernization Plan (draft). 11 April 1980. CCH Series XII.D.

(U) HF Target Studies, 1975, 1978. CCH Series XII.D.

(U) Morrison, John R. (Maj Gen, USAF, Ret.), personal and professional papers in CCH Series XI.R.

(U) "National Security Agency: The Evolution of a Centralized Response." CCH files, 1986.

(U) Pelton file. NSA General Counsel office.

(U) Rockefeller Commission Report and related correspondence. NSA Archives, acc nr 45146N, H07-0201-6.

(U) "Technology for Special Purpose Processors." March 1978. NSA Archives, acc nr 27451, CBUI 31.

7. (U) A few files and studies by SCE components were used. Available at AIA at Kelly AFB, San Antonio, are:

(U) "A Historical Monograph of the KAL 007 Incident."

(U) "A History of the USAFSS Airborne SIGINT Reconnaissance Program (ASRP), 1950-1977."

(U) "History of the Electronic Security Command." Annual. (Most are available in CCH Series X; others can be obtained from AIA, Kelly AFB, San Antonio, TX.)

(U) PL 86-36/50 USC 3604 "A Chronology of Significant Events in the History of the Electronic Security Command, 1948-1988."

(U) Whitacre, SMSgt Frank. "A Historical Study of the Drawdown of USAFSS Operations in Southeast Asia (SEA)." San Antonio: USAFSS, 1974.

8. (U) In contrast to Books I and II, outside scholarship played a big role in certain aspects of the current two books. As NSA's role has become more public, this source of information will inevitably expand.

Andrew, Christopher. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush.* New York: HarperCollins, 1994.

_____. "The Growth of the Australian Intelligence Community and the Anglo-American Connection," *Intelligence and National Security*, 4:2 (April 1989), 213-256.

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

Bernstein, Carl, and Marco Politi. *His Holiness: John Paul II and the Hidden History of Our Time.* New York: Doubleday, 1996.

Beschloss, Michael, and Strobe Talbot. *At the Highest Levels: The Inside Story of the End of the Cold War.* Boston: Little, Brown and Company, 1991.

Brzezinski, Zbigniew. *Power and Principle: Memoirs of the National Security Advisor, 1977-1981.* New York: Farrar, Straus, Giroux, 1983.

Burrows, William E. *Deep Black: Space Espionage and National Security.* New York: Random House, 1986.

Butler, David. *The Fall of Saigon.* New York: Dell Books, 1985.

Cline, Ray S. *The CIA Under Reagan, Bush and Casey.* Washington, D.C.: Acropolis Books, 1981.

Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy. Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM). New York: ACM, 1994.

Codevilla, Angelo. *Informing Statecraft: Intelligence for a New Century.* New York: Free Press, 1992.

Cole, Ronald H. *Operation Urgent Fury.* Washington, D.C.: JCS Joint History Office, 1997.

Congressional Quarterly. "The Iran-Contra Puzzle." Washington, D.C.: *Congressional Quarterly,* 1987.

Constance, Paul. "How Jim Bamford Probed the NSA," *Cryptologia,* 21:1 (January 1997), 71-74.

Dam, Kenneth W., and Herbert S. Lin (eds.). *Cryptography's Role in Securing the Information Society.* National Research Council, Computer Science and Telelecommunications Board. Washington, D.C.: National Academy Press, 1996.

Dobrynin, Anatoly. *In Confidence: Moscow's Ambassador to America's Six Cold War Presidents (1962-1986).* New York: Times Books Division of Random House, 1995.

Donnelly, Thomas, Margaret Roth and Caleb Baker. *Operation Just Cause: The Storming of Panama.* New York: Lexington Books, 1991.

Draper, Theodore. *A Very Thin Line: The Iran-Contra Affair.* New York: Hill and Wang, 1991.

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

Goldschmidt, Arthur. *A Concise History of the Middle East.* Boulder: Westview Press, 1979.

Greene, John Robert. *The Presidency of Gerald Ford.* Lawrence, Kansas: University of Kansas Press, 1995.

Guilmartin, John F. Jr. *A Very Short War: The Mayaguez and the Battle of Koh Tang.* College Station, Texas: Texas A & M Press, 1995.

Herring, George. *America's Longest War: The United States and Vietnam, 1950-1975.* Philadelphia: Temple University Press, 1986.

Hersh, Seymour. *The Price of Power: Kissinger in the Nixon White House.* New York: Summit Books, 1983.

_____. *The Target is Destroyed: What Really Happened to Flight 007 and What America Knew About It.* New York: Random House, 1986.

Johnson, L. K. *A Season of Inquiry: The Senate Intelligence Investigation.* Lexington, Kentucky: University of Kentucky Press, 1985.

Kagan, Robert. *A Twilight Struggle: American Power and Nicaragua, 1977-1990.* New York: Free Press, 1996.

Kahn, David. "Cryptology Goes Public." *Foreign Affairs*, Vol 58:1 (Fall 1979), 141-59.

_____. "Big Ear or Big Brother?" *New York Times Magazine*, May 16, 1976, 62-72

_____. "Soviet COMINT in the Cold War," *Cryptologia*, 1:18 (January 1988).

Karnow, Stanley. *Vietnam: A History.* New York: Penguin Books, 1983.

Kneece, Jack. *Family Treason: The Walker Spy Case.* Briarcliffe Manor, NY: Stein and Day, 1986.

Nelson, Dick, and Julie Koenen-Grant. "A Case of Bureaucracy in Action: The U.S. Embassy in Moscow," *International Journal of Intelligence and Counterintelligence*, Fall, 1993.

O'Toole, G.J.A. *Honorable Treachery: A History of U.S. Intelligence Espionage and Covert Action from the American Revolution to the CIA.* New York: Atlantic Monthly Press, 1991.

Peck, Winslow. "U.S. Electronic Espionage: A Memoir." *Ramparts*, August 1972, 36-50.

Persico, Joseph. *Casey: From the OSS to the CIA.* New York: Viking Penguin, 1990.

Ploss, Sidney I. *Moscow and the Polish Crisis: An Interpretation of Soviet Policies and Intentions.* Boulder: Westview Press, 1986.

Polmar, Norman, and Thomas B. Allen. *Merchants of Treason.* New York: Delacourte Press, 1988.

Powers, Thomas. *The Man Who Kept the Secrets: Richard Helms and the CIA.* New York: Alfred A. Knopf, 1979.

Prados, John. "The War Scare of 1983," *Military History Quarterly*, 9:3 (Spring 1997), 63-73.

Ranelagh, John. *The Agency: The Rise and Decline of the CIA.* New York: Simon and Schuster, 1986.

Shultz, George P. *Turmoil and Triumph: My Years as Secretary of State.* New York: Charles Scribner's Sons, 1993.

Smist, Frank. *Congress Oversees the United States Intelligence Community, 1947-1989*. Knoxville: University of Tennessee Press, 1990.

Spiegel, Steven L. *The Soviet-American Competition in the Middle East.* Lexington, Massachusetts: Lexington Books, 1988.

Talbot, Strobe. *Endgame: The Inside Story of SALT II.* New York: Harper and Row, 1979.

Theis, Wallace J., and James D. Harris. "An Alliance Unravels: The United States and ANZUS." *Naval War College Review*, Summer 1993, 98-123.

Theoharis, Athan. *Spying on Americans: Political Surveillance from Hoover to the Huston Plan*. Philadelphia: Temple University Press, 1978.

Toohey, Brian, and William Pinwill. *Oyster: The Story of the Australian Secret Intelligence Service.* Port Melbourne, Australia: Octopus Publishing Group, 1990.

Turner, Stansfield. *Secrecy and Democracy: The CIA in Transition.* Boston: Houghton Mifflin, 1983.

Walsh, Lawrence E. *Firewall: The Iran-Contra Conspiracy and Cover-Up.* New York: Norton and Co., 1997.

Weaver, Mary Ann. "Burying the Martyrs," *New Yorker*, January 1993.

White, Theodore H. *Breach of Faith: The Fall of Richard Nixon.* 1st ed. New York: Atheneum Publishers, 1975.

Woodward, Bob. *Veil: The Secret Wars of the CIA 1981-1987.* New York: Simon and Schuster, 1987.

9. (U) Material from the presidential libraries played a key role in this book. Those visited were:

Jimmy Carter Presidential Library, Atlanta, Georgia

Gerald R. Ford Presidential Library, Ann Arbor, Michigan

Ronald Reagan Presidential Library, Simi Valley, California

Index

25X6

PL 86-36/50 USC 3604

Doc ID: 4314472

Autodin (Automatic Digital Network), 141

Autosevocom, 142

Aviation Week, 124

Azorian (project name), 101

Bad Aibling, Germany (USM-89 PL 86-36/50 128-130, 132, 137-139, 208, 286, 307

Baker, Howard, 85, 92, 94

Baker Panel, 215

Bamford, James, 426-428

Bani Sadr, Abdul Hassan, 249

Bankhead (project name), 204

Ban Me Thuot, Vietnam, 3, 5

Banner, Roy, 85, 112

Barletta, Nicolas Ardito, 380

Barri, Nabith, 350-351

Barry, Ann, 265, 412

Bauded Signals Upgrade (project name), 192, 209-210, 215, 221-223, 411

Bayrum (project name), 301

Beachman (project name), 336

Beacon Hill, Panama, 200

Becker, Eugene, 166, 228, 311

Beecher, William, 101

Beijing, China, 227

Bell, Ernest, 291, 296

Bellfield, 143

Bell, Griffin, 104, 196

Bell Laboratories, 231, 291

Bendix Corporation, 151, 166, 308

Benhall, England, 136, 139, 287

Bennett, Donald, 87

Bracy, Arnold, 406

Bradlee, Ben, 415-416

PL 86-36/50 USC 3605

Breisach, Germany, 165, 306

Bremerhaven, Germany (USN-40), 27

Brezhnev, Leonid, 118, 122, 183, 255, 317

BROF (B Remote Operations Facility), 50-51, 166, 208, 214

Brooks, Jack, 99, 296

Brownell, George, 65

Brown, Harold, 222

Brzezinski, Zbigniew, 104, 148-149, 194, 196, 202, 231, 239, 255, 257, 260, 268, 270, 317

BSU – see Bauded Signals Upgrade

Buchwald, Art, 85

Bude, England PL 86-36/50 USC 3605 33, 135-136, 287, 393

Buffham, Benson, 15, 88, 162, 191, 228, 306

Bullseye (project name), 162, 340, 362-363

Bunker, Ellsworth, 202

PL 86-36/50 USC 3605

25X1, 6

Burchinall, Dean, 55

Burkhalter, Edward A., 281

PL 86-36/50 USC 3605

Burning Wind (project name), 353, 359, 372, 382, 390

Bush, George, 68, 122, 193, 230, 361, 383

Caddell, Pat, 260

Cain, James, 66

Cali Cartel, 363

Callaghan, James, 198