

~~TOP SECRET//COMINT//UMBRA~~  
~~TALENT KEYHOLE//X1~~

American Cryptology during the Cold War, 1945-1989 - Book IV

~~TOP SECRET//COMINT//UMBRA~~  
~~TALENT KEYHOLE//X1~~

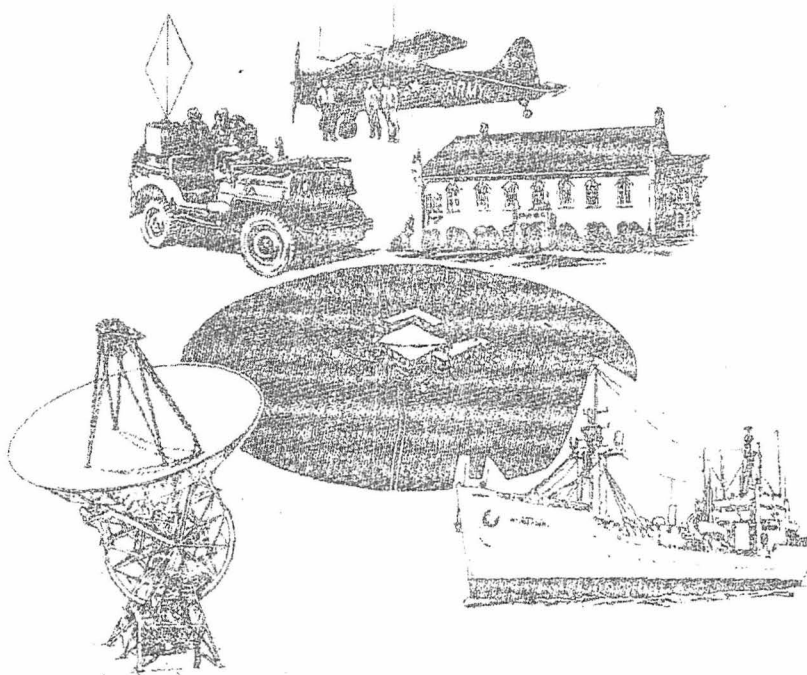
series VI  
volume 5

book IV

national security agency  
central security service

~~TOP SECRET//COMINT//UMBRA/TALENT KEYHOLE//X1~~

# UNITED STATES CRYPTOLOGIC HISTORY



## *(U) American Cryptology during the Cold War, 1945-1989*

### *(U) Book IV: Cryptologic Rebirth, 1981-1989*



Declassified Under Authority of the Interagency  
Security Classification Appeals Panel, E.O.  
13526, sec. 5.3(b)(3)  
ISCAP Appeal No. 2016-220, Doc. 1, Part 1  
Declassification Date: September 9, 2024

Derived From: NSA/CSSM 123-2  
Dated 24 February 1998  
Declassify on: X1, X5, X6



CCH-S54-99-01

~~TOP SECRET//COMINT//UMBRA/TALENT KEYHOLE//X1~~

**This monograph is a product of the National Security Agency history program. Its contents and conclusions are those of the author, based on original research, and do not necessarily represent the official views of the National Security Agency. Please address divergent opinion or additional detail to the Center for Cryptologic History (S542).**

**This document is not to be used as a source  
for derivative classification decisions.**

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

# **UNITED STATES CRYPTOLOGIC HISTORY**

*Series VI*  
*The NSA Period*  
*1952 - Present*  
*Volume 5*

*American Cryptology during the*  
*Cold War, 1945-1989*  
*Book IV: Cryptologic Rebirth, 1981-1989*

**Thomas R. Johnson**



**CENTER FOR CRYPTOLOGIC HISTORY**  
**NATIONAL SECURITY AGENCY**

**1999**

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

## Table of Contents

	Page
<b>(U) BOOK IV: CRYPTOLOGIC REBIRTH, 1981-1989</b>	
<b>(U//FOUO) Chapter 21: The Reagan Revolution</b>	
Background .....	263
The National Security Mechanism under Reagan .....	265
The Inman Appointment .....	265
General Faurer Becomes NSA's Director .....	266
The Odom Administration .....	267
At the White House .....	270
SIGINT Resources in the Reagan Years .....	271
The Cryptologic System in the 1980s .....	278
The FSCS Study .....	281
"Battlestar Galactica" .....	282
Comsat .....	286
25X1 .....	288
Cryptologic Communications .....	290
Cryptologic Computers .....	291
Computer Security .....	292
Operations Security .....	294
INFOSEC and the New Way of Doing Business .....	295
The Second Parties - the United Kingdom .....	299
Australia .....	302
New Zealand .....	303
Third Parties .....	304
25X1, 6 .....	306
All the Rest .....	307
<b>(U) Chapter 22: The Second Cold War</b>	
The SIGINT System and the Soviet Problem .....	315
The Polish Crisis .....	315
The Second Cold War .....	318
KAL 007 .....	320
Shemya .....	320
Misawa .....	321
Wakkanai .....	323
Tokyo .....	324
Washington .....	325
Moscow .....	328
New York .....	331
The Postmortems .....	332

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

Verification .....	334
The Relocatable Targets Problem .....	335
<b>(U) Chapter 23: The Rise of Terrorism and Unconventional Targets in the 1980s</b>	
Terrorism .....	345
The Dozier Kidnapping .....	347
The Sabana Seca Incident .....	349
Airline Hijackings .....	349
The <i>Achille Lauro</i> Affair .....	351
La Belle Discotheque .....	354
The War on Drugs .....	361
SIGINT and CounterIntelligence .....	365
<b>(U) Chapter 24: Military Crises and SIGINT Support during the Reagan Administration</b>	
Urgent Fury .....	371
The Falklands War – A Success Story .....	374
Just Cause .....	379
<b>(U) Chapter 25: Iran-Contra</b>	
Contra .....	387
The Nicaraguan Revolution and the Concern about Communist Subversion .....	387
Iran .....	392
<b>(U) Chapter 26: The Year of the Spy</b>	
Gunman .....	401
Prime .....	407
Pelton .....	409
Walker .....	417
Pollard .....	422
Hall .....	424
Carney .....	425
The Puzzle Palace .....	426
The American Library Association Suit .....	428
Epilogue .....	428
<b>(U) Glossary .....</b>	<b>433</b>
<b>(U) Sources .....</b>	<b>441</b>
<b>(U) Index .....</b>	<b>453</b>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

## **(U//FOUO) Chapter 21**

### **The Reagan Revolution**

#### **(U) BACKGROUND**

(U) Nineteen-eighty marked more than just a change of decade. It was a change of mood. Some have called it the Reagan Revolution. Reagan, a forever optimistic actor from California, came to office with a world view in complete contrast with that of the 1970s. He was tired of talk about limitations, wanted none of the gloom that had settled over the White House in the late Carter years. He would restore America's power in the world. He would start by spending the nation back into prosperity.

(U) When Gerald Ford left office, the national debt was \$644 billion. When Jimmy Carter departed, it was \$909 billion. When Ronald Reagan left office, it was more than 2 and one half trillion dollars. The severe gap between income and expenditures had a long-term impact on many areas of national life, not the least on the funding of defense programs.

(U) It was Reagan's dual approach that created the problem. He would generate demand by cutting taxes, but, paradoxically, he would increase spending on national defense. This would leave a gap between revenues and expenditures that would be made up by cutting domestic programs. But domestic programs could not be cut that much, and a considerable portion of the national debt came from the funding of defense programs.

(U) At the core of Reagan's defense revival was intelligence. It meant getting good information on adversaries, and it meant employing that information in active ways – a strong covert action program. The new DCI was a long-time Reagan friend, the manager of his successful presidential campaign in 1980 – William Casey. Casey's intelligence background was OSS in World War II. OSS had been excluded from COMINT during the war, and so to them intelligence meant HUMINT, i.e., agents. He had no experience with SIGINT, but he was a fast learner.

(U) When Casey became DCI, "technical intelligence" had just about taken over. The Carter administration believed in it, and most of the money went toward it. Despite the well-known Reaganesque proclivity toward agents and covert actions, this did not really change during his administration. His transition team wanted more money dumped into satellite programs, and the Reagan administration cut its sails in that direction from the first day.<sup>1</sup> Casey himself quickly came to understand the value of SIGINT, and did not share the institutional view of NSA that so dominated the thinking of his own staff. His own deputy, Bobby Inman, said later that

(U) For all of my difficulties with Bill Casey on so many other issues, on this one I would give him a clean bill of health....While he set out to rebuild and revitalize the DDO, he recognized the value of Signals Intelligence and the role it played....He did not bring an instinctively parochial view to the issue. Was it relevant? Was it timely? Was it useful? Did you need more money? These were the sorts of basic attitudes he brought.<sup>2</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

(U) William Casey and Ronald Reagan

(U) The Reagan administration marked the height of the Cold War. The president referred to the Soviet Union as the Evil Empire, and was determined to spend it into the ground. The Politburo reciprocated, and the rhetoric on both sides, especially during the first Reagan administration, drove the hysteria. Some called it the Second Cold War. The period 1982-1984 marked the most dangerous Soviet-American confrontation since the Cuban Missile Crisis.

(U) Despite the president's support of intelligence programs, NSA was wary. The White House viewed intelligence as a foreign policy tool, and used it to advance larger foreign policy interests, regardless of security implications. Three instances make the case.

~~(TS//SI-UMBRA)~~ In 1985, a Palestinian terrorist group captured an Italian cruise ship, the *Achille Lauro*, in the Mediterranean. SIGINT tracked the ship and its captors to Cairo and revealed plans by the Mubarak government to spirit their "problem" to Tunis. The capture of the terrorists was effected by a highly sensitive SIGINT source, and a leaky White House revealed the source.

~~(TS//SI-UMBRA)~~ The next year the Libyan bombing of a West Berlin night club, the La Belle Discotheque, led to the American bombing of Libya. The Libyan responsibility was revealed through intercept <sup>25X1, 6</sup> of Libyan state security communications.

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

Once again, SIGINT was exposed as the source, and the source dried up (at least temporarily).

~~(TS//SI-UMBRA)~~ The best known exposure of SIGINT since the Pearl Harbor hearings of 1945 had actually come in 1983, when the Reagan administration played the intercepted cockpit conversations of the Soviet pilot as he shot down KAL-007. The SIGINT gave the administration a tremendous foreign policy coup; the actual damage to SIGINT from the tapes was negligible. (But other information, from Gamma sources, may have done substantial damage.)

(U) There were numerous other instances. British historian Christopher Andrew cites just one – the 1988 exposure of the decrypt of Iraqi military communications relating to the Iraqi use of poison gas on their Kurdish population.<sup>3</sup> It came from an atmosphere in which the loss of sources and methods was deemed less important than the foreign policy gains.

(FOUO) Counterbalancing the Reagan administration's penchant for misuse of intelligence was the president's strong support of his intelligence agencies. In 1986 he became the first American president to visit NSA, as he gave the official dedication speech for NSA's two new buildings, Ops 2A and Ops 2B. He wanted to loosen the legal reins governing intelligence, and signed a new executive order, 12333, which gave NSA latitude in SIGINT collection that it had not had during the Carter years. Reagan revived the President's Foreign Intelligence Advisory Board (PFIAB), moribund under Carter. The new chair, Anne Armstrong, was a strong and effective advocate for the intelligence community.<sup>4</sup>

## (U) THE NATIONAL SECURITY MECHANISM UNDER REAGAN

### (U) *The Inman Appointment*

(U) Casey needed a deputy, and he was not inclined to go to the existing CIA structure. Thus the search turned outside CIA, and eventually settled on NSA director Admiral Bobby Inman. The way that Inman was selected became a Washington legend. His prime sponsor was Senator Barry Goldwater, who had urged that Reagan make Inman the DCI. As DIRNSA, Inman's reputation had become so special that he was regarded as essentially untouchable. Bob Woodward, in his book *Veil*, described Inman in the adulatory tone of the times:

(U) Inman knew the intelligence business cold. He was the best source on everything from the latest spy satellite to the bureaucratic maneuvering required to get intelligence programs going. He had a fabulous memory. With his boyish, toothy smile, large head, thick glasses, Inman looked like a grown-up whiz kid. He was one of the few intelligence officials who would talk to reporters and get them to hold off on stories that compromised intelligence. He had nurtured all the important relationships in the Congress. Goldwater could not recall an instance in which Inman had failed to return a phone call or to track down an answer on the rare occasion when he didn't know it.<sup>5</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

(U) Others in the news media had similar comments. According to the *Washington Star*, "It is reassuring both to those who want to see U.S. intelligence operations strengthened and to those who don't want to see the CIA crashing through the forest in its previous 'rogue elephant' role.... 'There is not a mark on him,' says a former admiral who worked with Inman in naval intelligence." At the Senate confirmation hearing, Senator Goldwater opened by saying: "You have my vote even before I hear your testimony...." Inman became the first superstar to emerge from NSA. Most expected him to maximize the role of SIGINT and to turn up his nose at covert operations and other messy programs.<sup>6</sup>

**(U) General Faurer Becomes NSA's Director**



(U) General Lincoln D. Faurer

(U) Inman's successor as DIRNSA was Air Force Lieutenant General Lincoln D. Faurer. Faurer had a strong flying background (he piloted both B29s and RB-47s) and experience in missile and space operations. Although he had no direct experience in cryptology, he had served two tours at DIA and three others in intelligence-related jobs. He came to NSA from Europe, where he had been both J2 USEUCOM, and deputy chairman of the NATO Military Committee. He thoroughly understood the intelligence needs of theater commanders, and he made support to military operations a central theme of his tenure at NSA.<sup>7</sup>

(U//FOUO) If Inman could be described as "brilliant and brittle," "Linc" Faurer might have been accurately depicted as avuncular but determined. He valued accommodation and collegiality, and he tried to reconstruct

NSA's management system based on new management principles emphasizing cooperation and corporate decision-making.<sup>8</sup> It was difficult to redirect NSA's staff system in such a radical way. Under Inman, management had been top down, and Inman neither needed nor wanted a staff system. Faurer was just the opposite.

~~(S//SI)~~ Much of Faurer's energy was directed toward sharpening support to military operations. As the former deputy chairman of NATO's Military Committee, he focused on SIGINT support to NATO, establishing a semi-annual meeting<sup>25X1, 6</sup>

This mechanism violated the strict bilateralism of Third Party relationships codified in the UKUSA Agreement, but that approach had been growing outmoded anyway. Multilateralism was the only feasible approach in the NATO environment.<sup>9</sup>

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~(S//SI)~~ Much of his effort along this line was doomed to frustration. During the Grenada operation, NSA was shut out of operational details (see page 372), bringing the dispute over this long-running problem to a boil. After the bombing of the Marine barracks in Lebanon in 1983, the Navy insisted that SIGINT support to the remaining Marines be routed through Sixth Fleet. Faurer, experienced in the ways of military operations, rejected that approach. "We fought that battle and it got more heated after the bombing than it did before and it's dead wrong. I mean, you just can't live with it that way." He cultivated his relationships with the J3 (chief of the JCS operations staff) throughout his tenure, trying to educate each successive occupant of the chair, and he got understanding nods but no results. "And it went on the entire time. We never solved the problem."<sup>10</sup>

(U//FOUO) Faurer developed a high regard for both his bosses, Casey and Weinberger. As for Casey, once Faurer got over the difficulty of understanding what he was saying (a problem that followed Casey his whole life - unintelligible speech), he acquired great respect for the DCI. "I happen to think Bill Casey is as fine a DCI as we've had in the time I've been associated with intelligence, and I go back to Jim Schlesinger."<sup>11</sup> But Faurer read his own charter literally, and believed that in DoD, his direct supervisor was Weinberger. He never accepted the delegation of NSA to the deputy secretary of defense, William Taft. Faurer fought Taft constantly to insure that NSA's national role remained an independent responsibility. They had disputes over NSA's national role in policy issues and over budget issues that transcended the Defense Department. They were never resolved, and Faurer was actually fired at Taft's behest over a now-obscure budget issue several weeks prior to the agreed-upon retirement date. General Faurer, a bulldog to the end, went down fighting for what he believed in.<sup>12</sup>



(U) Caspar Weinberger

#### (U) The Odom Administration

(U//FOUO) Faurer's replacement in 1985 was a former armor officer who had become one of the Army's top Sovietologists. William Odom had had a tour at the Potsdam mission in the mid-1960s. The Potsdam mission was one of the best training grounds for attaché work, and it was followed six years later by a tour as assistant Army attaché in Moscow.

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

Odom was exposed to SIGINT, especially in Moscow, and over the years he developed a keen appreciation for the interplay of intelligence disciplines.<sup>13</sup>



(U) General William Odom

(U) When Zbigniew Brzezinski became Jimmy Carter's national security advisor, he plucked his former student, William Odom, out of the Army to serve on his staff. Said Brzezinski, "I knew him from an earlier association with me at the Research Institute on International Change at Columbia, I respected his views on Soviet military affairs and strategy, and I considered him to be an innovative strategic thinker."<sup>14</sup>

(U) After four years in the White House, Odom had gone on to serve as the deputy assistant chief of staff for intelligence in the Pentagon, and soon took over as the ACSI.<sup>15</sup> His broad exposure to Army intelligence made him a prime candidate to succeed Faurer. And the Army had not had a director since Marshall Carter departed in 1969.

(U//FOUO) Odom brought a unique personality to the job. According to his deputy, Robert Rich, he was a good listener and a reasonable person to work for, who could

examine the intellectual facets of a decision and come up with the right answer. But he did not project this image. What most NSAers remember was a different Odom: "...ready, fire, aim; loud, boisterous, ranging over all kinds of intellectual territory, strategy of the nation, strategic concepts, tactical concepts."<sup>16</sup> Many felt that he suffered from the typical disease of ivory tower intellectuals – hearing one voice only: his own.

(U//FOUO) Odom had a different perspective on NSA. He likened the job to that of commanding a specified command. It had, he liked to point out, operational control over three service components, a worldwide scope of operation, its own logistics system, its own training school, a unique research and development organization, its own procurement system, and so forth. Next to the DCI, it was the most powerful job in American intelligence.<sup>17</sup>

(U//FOUO) For a specified command, though, it lacked certain essentials. Most prominently, NSA had no staff system analogous to that of a military command. Without a staff, the director simply had to accept the judgments of his deputy directors, and had no independent means of managing actions or verifying information. It was a consequence of historical evolution at NSA, and it fitted NSA's unique way of doing business. Odom

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

battled the system his entire time at NSA, but felt that he never changed the way NSA operated.<sup>18</sup>

(U//FOUO) What NSAers remembered most distinctly from the Odom era were the Ten Thrusts (see Table 18). Originally written by Odom himself, these began as six thrusts relating to SIGINT, and focused primarily on maintaining NSA's edge in various technical disciplines such as cryptomath and in sharpening the focus of customer support. Harry Daniels, the DDI, took immediate exception to a list of thrusts which excluded INFOSEC issues, and submitted his own. Odom struck one of the original six from the list and added Daniel's five, to come up with a nice round number. It was a good list, just right for the mid-1980s. Odom did seem to understand the business.

~~(S//SI)~~ Table 18  
General Odom's Ten Thrusts

1. Modernize the SIGINT collection and processing systems to cope with the changing target communications technology.
2. Integrate tactical and national SIGINT capabilities to satisfy more effectively military requirements in peace, crisis, and war.
3. Maintain and improve our capabilities to support diplomatic, economic, and other nonmilitary requirements for SIGINT support.
4. Maintain a large U.S. lead in cryptanalytic capabilities (both computer capability and personnel).
5. Design a framework for a survivable SIGINT system, under all conditions, including general war, which we acquire incrementally and through astute dual-use applications over the next decade.
6. Provide easily attainable, inexpensive, user-friendly Information Systems Security features.
7. Speed up research for major breakthroughs in the technology of computer security; at the same time, help industry manufacture more "trustworthy" computer products for defense and other government needs.
8. Establish a program to reduce significantly the HUMINT threat to Information Security Systems.
9. Provide modern, secure, user-friendly key management systems.
10. Remove the COMSEC block obsolescence condition by the end of 1991 and establish a program to protect against this condition in the future.

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~(S//SI)~~ The most controversial thrust was to insure a survivable system. Fashioned during the Second Cold War, it made a lot of sense at the time. It became known eventually as Triangle, the project to insure the survival of the cryptologic system in wartime. Much of Triangle involved decentralization of the process. The Triangle plan used such then-unfamiliar terms as Theater Support Nodes and Regional SIGINT Support Centers. Funding Triangle amounted to the diversion of large amounts of money for a concept that many in NSA thought to be unnecessary. According to his successor, Rear Admiral William Studeman, there was a tendency at NSA to try to wait out the Odom directorship in hopes that Triangle would simply go away.<sup>19</sup>

(U//FOUO) Like Faurer, Odom worked for two bosses, Weinberger and Casey, but he managed the trick with aplomb. Within DoD he generally reported directly to the secretary of defense but, aware of the Faurer-Taft confrontations, carefully kept William Taft in the loop with occasional briefings. His real affinity, however, was clearly for Casey. The two got on well together, and Odom held Casey in high respect for his substantive knowledge of intelligence issues and his ability to deal with them off the cuff. They formed a united team in 1986 to try to stop the press from publishing leaks that damaged intelligence sources and methods.<sup>20</sup>

#### **(U) At the White House**

(FOUO) NSA still enjoyed a special relationship with the White House. After a brief and fitful flirtation with the idea of bringing someone from State Department in to run the Situation Room, Richard Allen, the first of a long line of Reagan's national security advisors, chose NSAer ~~PL 86-36/50 USC 3605~~ as his Situation Room chief. ~~PL 86-36/5~~ stayed during the first Reagan administration, long enough to get a clear picture of how intelligence issues were handled.

(U//FOUO) Under Carter, intelligence and national security topics got a highly organized, if somewhat egocentric, direction from Brzezinski. But this process never got started under Reagan. The leaks, the employment of SIGINT to push a foreign policy agenda, the disjointed way in which intelligence in general was treated (culminating in the Iran-Contra imbroglio) was a true bill of the process. For in fact, there never was a process under Reagan.

(U) Reagan modeled his White House administrative procedures after Nixon, with a strong staff chief, Edwin Meese. Everything was routed through Meese, and even Richard Allen contacted the president through him. This cut off the president from direct access to intelligence, and when Allen departed he had never been able to establish a relationship with Reagan. His successor, Judge William Clark, accepted the job only on condition that he enjoy access to the president, but the damage had been done, and during the first Reagan administration the White House never had a strong national security advisor, nor did it ever have a system in which tailored, focused intelligence arrived in the Oval Office. The job became a revolving door, with first Allen, then Clark, then Robert McFarlane, John Poindexter, and finally Frank Carlucci, cycling through. According to ~~PL 86-36/5~~ the

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

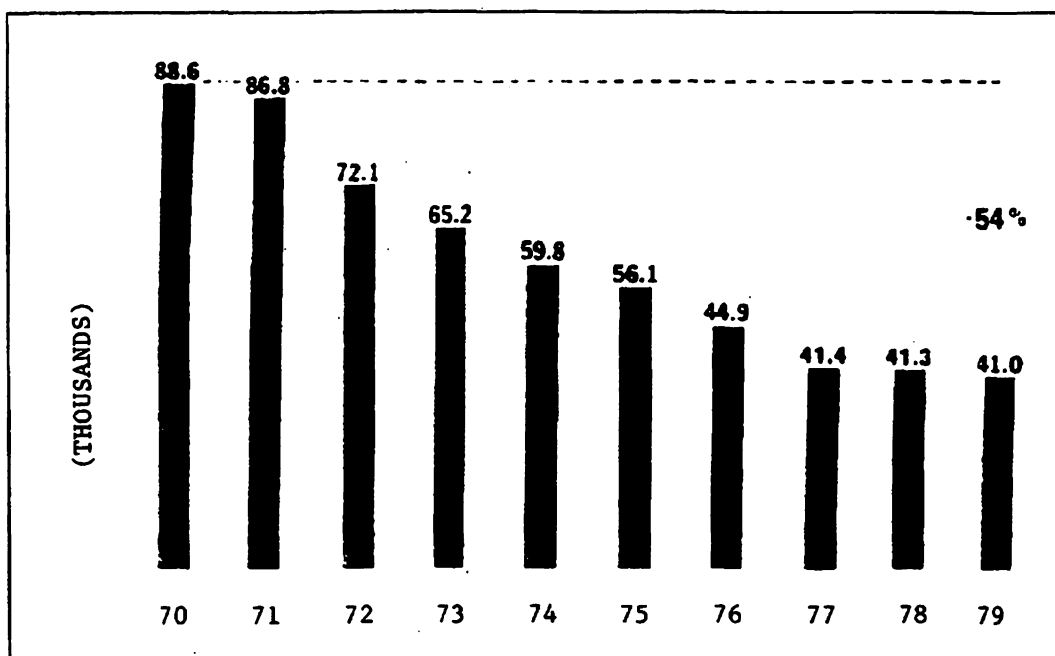
~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

process, if there was a process, lacked substance, and difficult intelligence issues were dealt with in a superficial way.<sup>21</sup>

#### (U//FOUO) SIGINT RESOURCES IN THE REAGAN YEARS

~~(C)~~ Ronald Reagan inherited a cryptologic system in parlous shape. Manpower over the previous decade had dropped from 88,600 to about 41,000 (see Table 19). At first glance, money appeared to be on the increase, but that was before inflation was factored in. The 1970s was a decade of high inflation, and the gap between current and constant dollars had widened progressively through the ten years (see Tables 19 and 20).

~~(C)~~ Table 19  
Cryptologic Manpower, FY 1970-FY 1979<sup>22</sup>

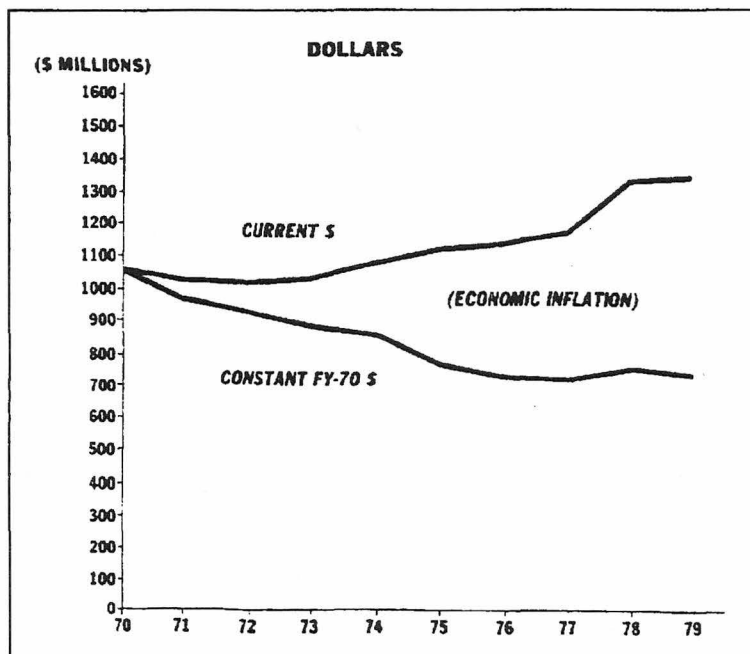


~~(S)~~ The Reagan administration began pumping money back into intelligence programs. From the 1980 through 1986 fiscal years, the overall cryptologic budget rose 152 percent (see Table 21), a breathtaking ascent unmatched since World War II. The most spectacular growth was in overhead systems, which by 1988 had become fully 43 percent of the total SIGINT pot.<sup>24</sup>

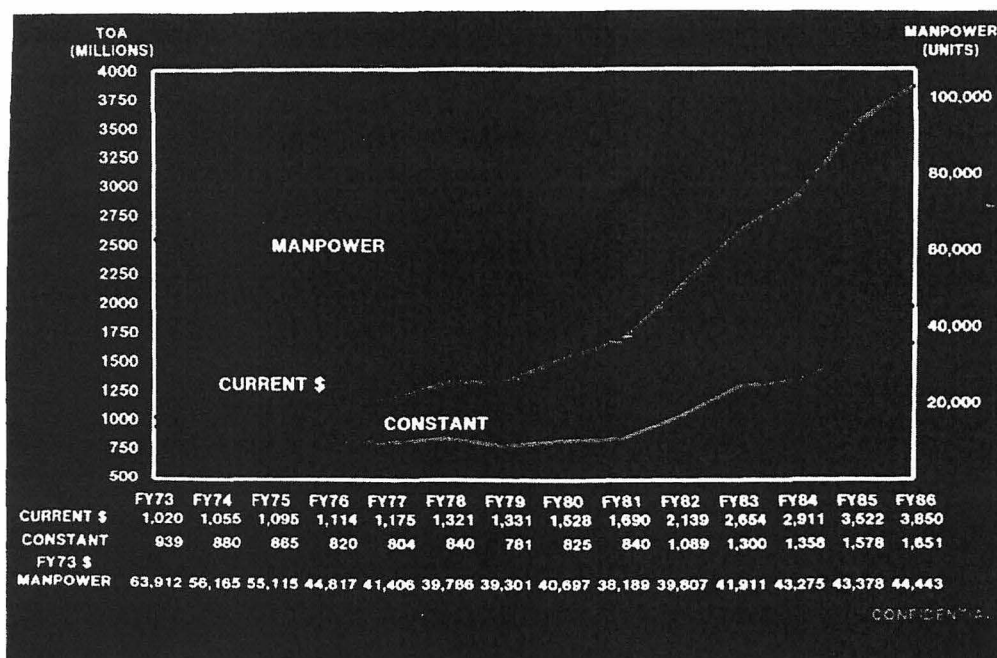
~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~(C)~~ Table 20  
CCP Funding  
During the 1970s <sup>23</sup>



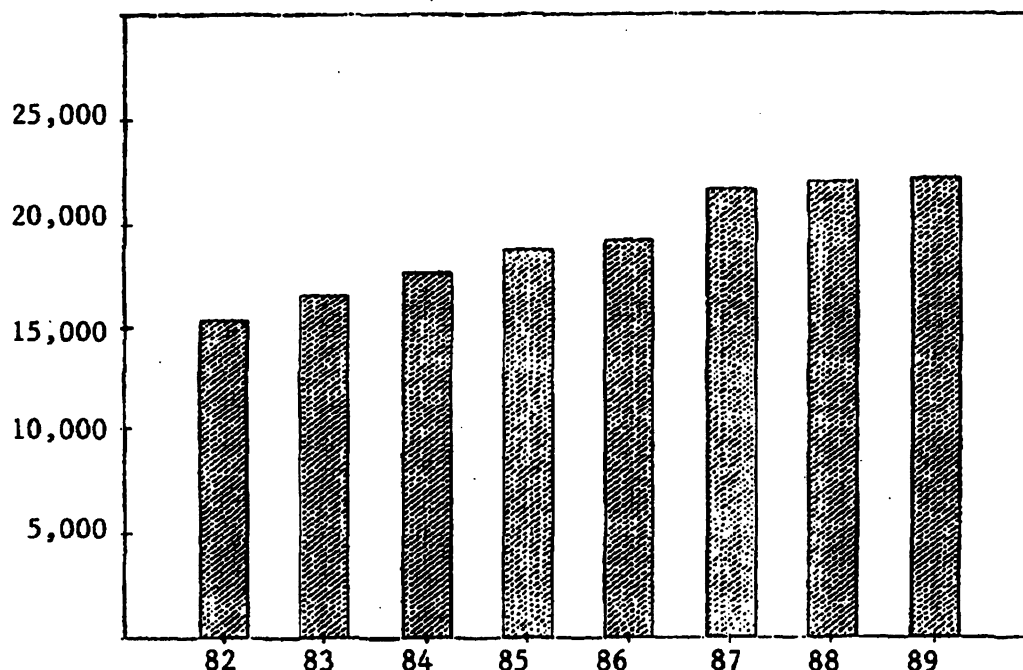
~~(C)~~ Table 21  
The Cryptologic Budget, FY 1973 Through FY 1986 <sup>25</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

(C) Along with money came people - lots of them. NSA's total population rose by 40 percent during the 1980s. Beginning with 19,018 in 1983, the Agency's population peaked in 1990, just before the collapse of the Soviet Union, at a total of 26,679. The dramatic rise was across the board, civilian and military, but was most pronounced on the civilian side (see Table 22). While the military component rose 24 percent, the civilian side increased by 46 percent.<sup>26</sup>

(C) Table 22  
NSA's Full-Time Civilian Strength, 1982-1989<sup>27</sup>



(U) Almost a thousand billets came to NSA in 1986 as the result of a decision by the General Services Administration to turn over support operations. Part of a broader plan to relinquish maintenance to single-tenant government-owned facilities, the GSA plan for NSA involved both maintenance (542 billets) and security guards (381 people). In October of 1985 Terence Golden, administrator of GSA, met with General Odom, and in April of 1986 Odom formally accepted the plan.<sup>28</sup>

(U) The hiring glut took place mostly at the lower grades, but NSA's average grade level stayed in the range of GG-10, substantially higher than the government-wide average. What took place to level it out was rapid promotions. The 1980s saw a major surge in promotions, with a dramatic spike in fiscal year 1985. But the downside was the slide in average experience level, as new hires replaced old hands.<sup>29</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

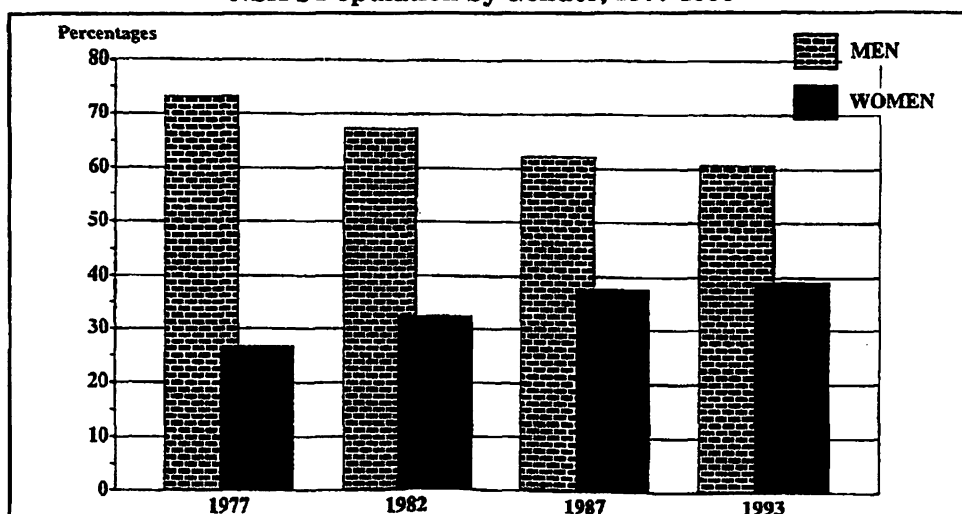
~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

(U//FOUO) In the light of the rapid civilian hiring program, the military contribution to cryptology became a source of concern. As the percentage of the military population declined, its influence would also inevitably decrease, along with military cryptologic experience levels. This could unfavorably impact support to military operations. Moreover, rapid civilian hiring was taking place primarily out of colleges, and military conversions, once a dominant source of civilian manpower, had declined by 1982 to 6.7 percent of all hiring actions. In 1988 Dr. James Donnelly headed a panel that looked at military manpower in the cryptologic system. Donnelly's main concern was the increasing congregation of military billets at the front end of the system, leaving very few at NSA, where much of the "technology transfer" had to take place.<sup>30</sup>

~~(C)~~ The fastest-growing segment of NSA's population during the 1980s was actually the part-time work force. A product of the Carter administration, the part-time segment grew from 330 in fiscal year 1981 to a peak of 1,044 in 1990. This explosive growth outstripped all other hiring areas, and a significant percentage of hiring actions (8.7 percent in fiscal year 1982) came from part-time to full-time conversions. One major reason for the increases in part-time employees was that NSA management discovered that they did not count against the Agency's official strength. It was thus a way to increase personnel without appearing to do so.<sup>31</sup>

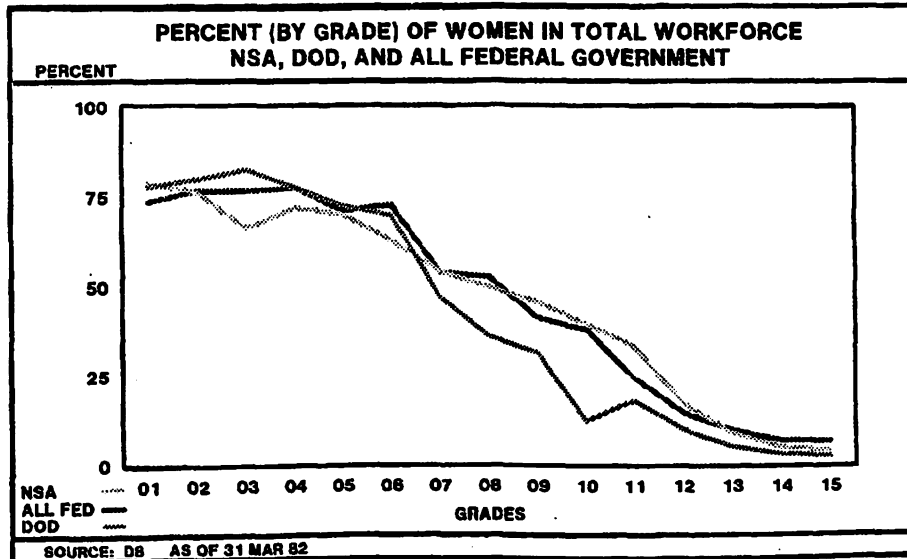
(U) As the work force grew, so did the percentage of women and minorities on the rolls. From 1977 to 1993, for instance, the percentage of women at NSA grew from about 26 percent to 39 percent (see Table 23). But the percentage of women by grade declined dramatically as grade rose, even though the decade opened with NSA's first female deputy director, Ann Caracristi. Women constituted a majority up through grade eight, but at that point the chart dipped dramatically, and women made up less than five percent of the grade fifteens. This compared closely with the overall government statistics, as Table 24 shows.

~~(C)~~ Table 23  
NSA's Population by Gender, 1977-1993<sup>32</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

(U) Table 24  
 Percentage of Women by Grade at NSA, DoD and Federal Workforce<sup>33</sup>



(U) The concentration on college-level hiring increasingly tipped the scales toward a more highly educated workforce. In the ten fiscal years from 1972 to 1982, for instance, the percentage of employees with college degrees increased 24 percent, while those with advanced degrees increased 125 percent. Those with less than two years of college actually declined by 22 percent.<sup>34</sup>

(U) More people required more space. And as personal computers became more common (during the decade 70 percent of the workforce was provided with a PC), people tended to require larger offices. So NSA launched an unprecedented building boom which resulted in the addition of 240,000 square feet per year during the decade. Much of it was leased space. The International Tower Building came under an NSA lease in 1980. The following year the Agency began leasing the new Airport Square buildings, which were replacing woods and fields in the vicinity of the FANX complex at BWI.

That same year General Faurer broke ground on Ops 2A and Ops 2B, which were dedicated by President Reagan five years later. In 1990 the new Research and Engineering building was dedicated, to add to the Special Processing Lab (opened in 1988) and numerous leased facilities in the general Fort Meade vicinity. (see Table 25)<sup>35</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~





(U) Construction of Ops 2A

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

(U) Dedication of Ops 2A and 2B by President Reagan

(U) One solution to the space problem was to go upward. In 1983 NSA awarded a contract to American Seating Company to provide and install systems furniture, which would permit the workforce to add personal computers and other office aids without increasing floor space per person. The original contract provided for some 8,000 workstations at a price of about \$5 million. But it was only the beginning, and by 1993 approximately 20,000 workstations had been installed at a cost of \$60 million. This improvement came in the late stages of an earlier movement to provide raised flooring. Begun in the basement of Ops-1 in the 1960s, raised flooring was originally installed only in rooms with computer mainframes. As smaller computers took over the Agency, people got tired of tripping over cables strung across tile floors from one machine to another. Slowly, workspaces were vacated and raised flooring installed. By 1993 some five million square feet of raised flooring had been installed in NSA buildings at Fort Meade. It not only got unsightly and potentially dangerous electrical cables off floors; it had the attendant benefit of providing carpet tiles, which reduced noise (and looked nicer).<sup>37</sup>

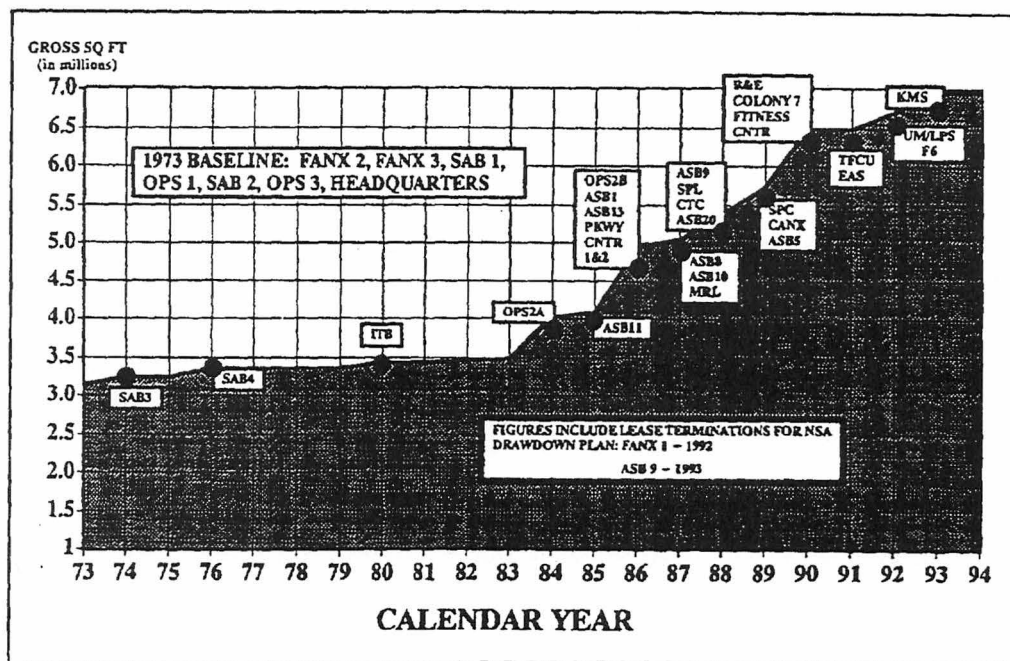
(U) In the early days Fort Meade had been serviced (excepting only the Baltimore-Washington Parkway) by narrow, winding roads going east and west to bedroom suburbs

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT UMBRA/TALENT KEYHOLE//X1~~

(U) Table 25  
Growth of NSA Space from 1973 to 1994



of Severna Park, Glen Burnie, Laurel and Columbia. The drive to either Severna Park or Columbia commonly took half an hour or more, much of it spent waiting in a long snake of cars twisting through the Maryland countryside. With NSA population projections going virtually through the roof, NSA began looking at an environmental overhaul. In the early 1980s the State of Maryland began widening Route 32 both toward the east and west. It was called the Patuxent Freeway project, and as sections became functional in the late 1980s and early 1990s, traffic congestion around Fort Meade declined (but didn't go away).<sup>38</sup>

#### (U) THE CRYPTOLOGIC SYSTEM IN THE 1980s

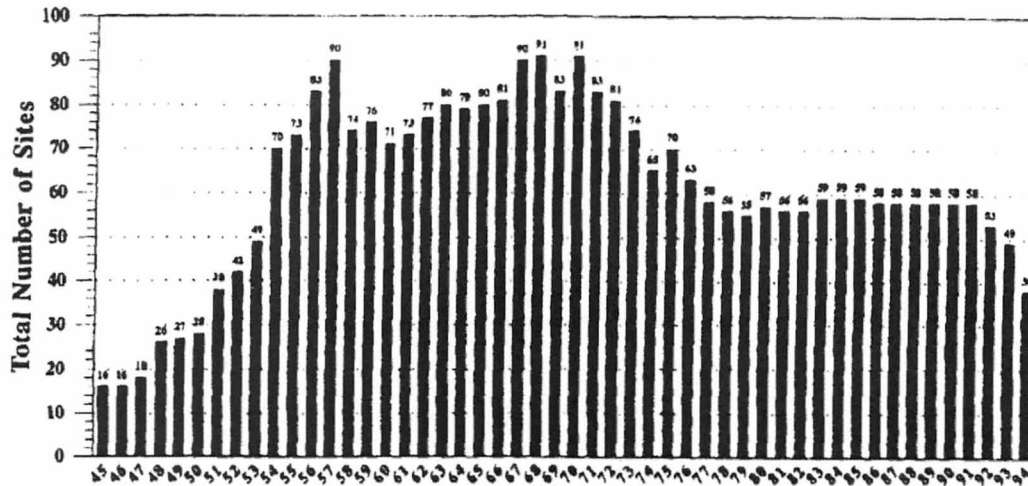
~~(S//SI)~~ The 1980s were the decade when NSA's reliance on HF collection finally came to an end. Rumors of its death, greatly exaggerated for many years, caught up with reality early in the decade. The cryptologic field system began the 1980s at the bottom of a ski slope (see Table 26). But the money that Reagan pumped into the system did not appear to benefit that system. The size of the conventional field site system stopped declining, but remained flat throughout the decade.

~~(S//SI)~~ The Army was hardest hit by the reductions of the 1970s. In 1972, ASA had eighteen field sites; a decade later, only nine. Gone were five sites in Southeast Asia and

~~TOP SECRET//COMINT UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

(C) Table 26  
Cryptologic Field Sites, 1945-1994

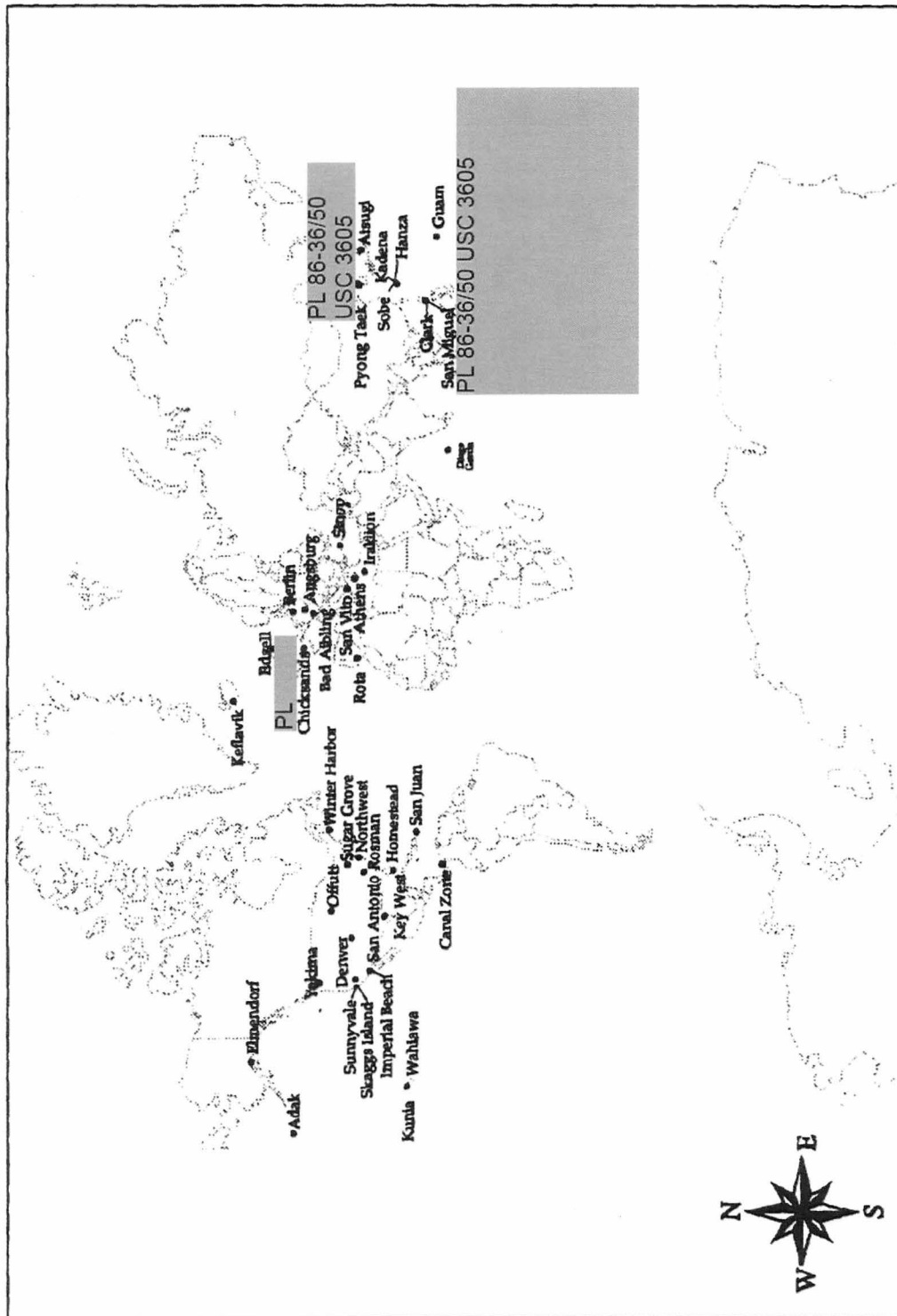


three in Germany, plus scattered locations in Ethiopia, Taiwan, Virginia and California. The only true addition was the INSCOM component of the cryptologic conglomerate at Kunia. To a degree this reflected the fact that Army SIGINT collection was the least technologically sophisticated of the services (see map page 280).

~~(S//SI)~~ Air Force field sites also dropped dramatically, from twenty-six in 1972 to only fifteen a decade later. Security Service lost three sites in Southeast Asia, while base consolidations in Germany and Japan resulted in the closure of four sites. Political forceouts in Turkey and Taiwan caused three site closures. If Security Service base closures were not as severe as with ASA, it was due in large part to the fact that the Air Force sites, and targets, were more technologically sophisticated. Security Service was thus better positioned to maintain its collection posture against modern communications. The Navy was least affected, at least in terms of numbers of sites. Thirty field sites in 1972 declined to twenty-seven ten years later.

~~(S//SI)~~ The field system was growing only in terms of joint and NSA-managed sites. Seven sites in 1972 had expanded to eight, despite the loss of two sites, in Asmara (lost during the Ethiopian Revolution of 1975) and Shemya, Alaska. Two PL 86-36/50 sites, PL 86-36/50 and Rosman, appeared, along with a joint Army-Air Force wideband site at San Antonio, Texas. The growth in this area was indicative of where the money was going - to high-tech collection.

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



(S//SI) Field site locations as of 1986

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~**(U) The FSCS Study**

~~(TS//SI//TK)~~ In 1983 NSA began a study of the increasing cost of the system programmed as the replacement <sup>25X1</sup> [REDACTED] Called the NSA ELINT Overhead Mix Study, its conclusions caught the attention of the DCI and Congress, and in December of that year Vice Admiral Burkhalter, director of the Intelligence Community Staff, established the Future SIGINT Capabilities Study (FSCS). Burkhalter broadened the study to the entire SIGINT system. The objective was to match existing and programmed systems against assumed target changes and to identify the gaps. Phases I and II would look at everything but Overhead; Phase III would address only satellites.<sup>39</sup>

~~(C)~~ The resulting documents highlighted the increasing technological sophistication of the targets, and they marked a watershed of sorts. It was no longer possible to think of the SIGINT system in the same terms as professional cryptologists had thought of it since World War I. The HF system had become secondary to more sophisticated collection in the higher frequency ranges.

~~(S//SI)~~ The study focused on target changes that would affect collection and processing. Increasingly sophisticated target cryptography took a place on the "threat list," but only a minor place. The major threats were high data rates, digitization (as opposed to the more traditional analog signals), low probability of intercept techniques like frequency hopping and spread spectrum, the use of wider bandwidths and higher frequency ranges, advanced radar techniques, and the growing use of communications satellites. The study's conclusions depicted a communications target that centered on almost everything but HF manual Morse communications.

~~(TS//SI//TK)~~ The existing SIGINT system was deficient in almost every capability. It would need to migrate to <sup>25X1</sup> [REDACTED] and to SIGINT satellites that could access communications, like microwave and military multichannel systems, deep in the heart of the target countries. The volumes would be so huge that front-end filtering and processing prioritization would be essential. <sup>25X1</sup> [REDACTED]

<sup>25X1</sup> [REDACTED]

<sup>25X1</sup> [REDACTED] SIGINT satellite geolocation must be improved and its reach expanded. SIGINT satellite systems like <sup>25X1</sup> [REDACTED] would have to work together in an interlocking mode to achieve the needed geolocation capability.

~~(S//SI)~~ Though FSCS concentrated on hardware and software, it did stray into manpower implications. Despite the contraction of the traditional HF field collection system, the workforce would have to grow to handle the massive volumes of material to be processed. Moreover, the skill mix would move rapidly into high-tech areas, and the people hired would be engineers, cryptomathematicians, and computer systems designers. The armed services did not produce people like that - NSA would have to hire increasingly from colleges or private industry to find the kinds of people it needed. Retention would be more difficult as NSA would have to compete with private industry for college-trained

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

technical people. The federal salary structure simply could not compete in these areas – job satisfaction would have to be the carrot.<sup>40</sup>

~~(TS//SI//TK)~~ To a workforce of the late 1990s grown accustomed to the new communications challenges, this sounds very familiar. In the mid-1980s, it was visionary. The FSCS study spawned a plethora of committees looking at various aspects of the problem. One committee predicted that the cryptologic system would require some \$20 billion more money in the CCP base through 2000 in excess of what had already been funded. At field sites alone, \$11 billion would be needed to deal with complex signals, while the need for system survivability would require another \$3.6 billion. Satellite systems would require expanded frequency coverage and increased geolocational capability. Computer systems had to change to defeat Soviet encryption technology. The only area where money could actually be saved was in the satellite programs themselves. There, the plan was to combine the three SIGINT satellites <sup>25X1</sup> into a single follow-on system.<sup>41</sup>

**(U) "Battlestar Galactica"**

~~(TS//SI//TK)~~ The plan for an overall SIGINT system was dependent on the resolution of an ongoing donnybrook over overhead resources. The dispute centered on the three competing SIGINT collectors downlinking to <sup>25X1, 6</sup> and Denver <sup>25X1</sup>. The rival systems had evolved over time in response to crash requirements, and each had a separate sponsor and separate constituencies. Many who had been involved in the birth of the three systems acknowledged the illogic of competition at that level, and some dreamed of amalgamating them into one program.

~~(TS//SI//TK)~~ Program A, the <sup>25X1</sup> was an Air Force program in which NSA was a close partner, and Lockheed Missile and Space Corporation was the prime contractor. Program B was the CIA program, and its prime contractor had always been TRW. CIA pushed for a single system, and in December of 1985 the DCI, William Casey, decreed that the FSCS study group would operate under the assumption that the system would evolve into a single, one-system-does-all program. It would replace five programmed <sup>25X1</sup> and <sup>25X1</sup> satellites with four satellites operating within an integrated system. The major competitors, Lockheed and TRW, would submit proposals for the consolidated system. The stakes would be huge – the winner would emerge with the entire geostationary SIGINT satellite program, while the loser would become a subcontractor. The <sup>25X1</sup> system, being a highly elliptical program essentially different from a geostationary system, was not to be modified. The proposed system was so grandiose that it was referred to by Admiral Inman as "Battlestar Galactica."<sup>42</sup>

~~(TS//SI//TK)~~ The outlines of the new system were revolutionary. It would eventually downlink to a single ground station in the continental U.S., which would distribute signals to various processing locations for customized follow-up. Signals would be relayed through communications satellites to the ground station, thus allowing a satellite to communicate with a location beyond the radio horizon and freeing SIGINT satellites from the geographic

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

tether that had always limited them. 25X1

25X1

25X1

Much attention would be paid to improved geolocation accuracy and better crosslinking among the satellites. Satellites would have better receivers with more flexible tuning options. The four balls would be launched from 1992 to 1995; the program cost would be \$9.5 billion, including \$1.1 billion for improved SIGINT processing.<sup>43</sup>

~~(TS//SI//TK)~~ The first satellite in the series would be launched 25X1 and would 25X1, 6 which would become the interim control and processing center. 25X1 would be positioned as needed in 25X1 nodes, and would have 25X1 which would be called Gateway. This center, whose location had not been chosen 25X1 were both candidates). would take satellite control 25X1, 6 and could manage the entire system. 25X1 would be the initial 25X1 (similar to the role for 25X1, 6 and 25X1 would be the backup, 25X1, 6 as a system location.<sup>44</sup>

~~(S//SI//TK)~~ NSA, being the signal processing organization, participated in all the system discussions and studies. The Agency generally kept its political opinions to itself, confining its advice to technical assessments of the feasibility of various approaches. Robert Hermann, director of NRO in the early 1980s, once said "NSA didn't care, shouldn't have cared."<sup>45</sup> But under the surface there was growing concern at the Agency about costs. An NSA advisory board wrote to General Odom in July of 1985 that SIGINT satellite costs in the National Reconnaissance Program were growing so fast that they could squeeze out some favored programs in the CCP. It would be a good idea to get a handle on satellite program costs, and soon.<sup>46</sup>

~~(S//SI//TK)~~ In fact, NSA's role in the overhead system was not so sterile as it appeared from the outside. Within the vortex was a fierce bureaucratic battle to control the SIGINT satellite business. Part of this undoubtedly stemmed from the philosophy of SIGINT management that NSA had always lived by. In the United States, SIGINT was monolithic, and control was vested in a national manager. But the overhead business was controlled by the NRO, and when NSA tried to intervene, either to manage the satellite planning and programming, or to exercise day-to-day direction over satellite operations, it was on NRO's turf.

~~(TS//SI//TK)~~ But viewed from NSA's perspective, the issue revolved around a management system that was inefficient from a cost standpoint. NSA managers believed that NRO was paying far too much to its favored contractors for satellite system design, launch and operation, and that this was impacting on money that should have been available for other SIGINT programs. Moreover, if NSA people could control mission ground site operations, they would have a much more responsive system, and could order satellite collection priorities according to the requirements of the entire SIGINT system. In 1981, Admiral Bobby Inman approached former NSAer Robert Hermann, then the director of NRO, to get a change in the rules by which spacecraft were controlled. From the strong-

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

willed Inman's standpoint it made perfect sense to control spacecraft operations from NSA, but an equally strong-willed Hermann told the NSA director that if NSA controlled the programs it would have to fund them, which meant taking the heat in Congress for a large slice of the NRO budget. There was no resolution of the dispute, and the management of SIGINT satellites remained as it had been.<sup>47</sup>

~~(TS//SI//TK)~~ Despite disagreements at the top, NSA and NRO managed to cooperate in the creation of a new system tasking center, the Overhead Collection Management Center (OCMC). It resulted from a July 1983 conference between William Kvetkas (chairman of the SIGINT Committee), Robert Rich (deputy director of NSA) and Jimmy Hill (deputy director of NRO). Kvetkas could not secure agreement even in such a small group, so he wrote a memo to John McMahon (deputy DCI) proposing a new joint tasking center on the DEFSMAC model. (Attached to the memo was a two and a half page nonconcurrence from Hill.) Kvetkas presented McMahon with three options, and McMahon selected one which created an OCMC at NSA headquarters, and permitted DIRNSA to name the director, the director of NRO to name the deputy, and the DCI to name the chief of requirements. This permitted conflict resolution at a technical level, and resulted in a joint organization that soon proved its worth.<sup>48</sup>



(U) George Cotter

~~(TS//SI//TK)~~ Disputes over satellite system control continued into the program. NSA wanted to be the host for the eastern gateway that would replace <sup>25X1, 6</sup> while NRO demanded to exercise its customary host role. NSA wanted to handle system programming and acquisition, not just the ground processing equipment. NSA wanted to handle site and operations security, but NRO, which had always controlled overhead security, forcefully rejected this and all other NSA proposals.<sup>49</sup> In fact, NSA proposed nothing less than a revolution in the way SIGINT overhead systems were handled. The most extreme view, promoted by Agency senior George Cotter, melded the satellite business into the U.S. SIGINT system. NSA would plan, program and acquire SIGINT overhead systems; it would budget for all overhead systems; it would manage contracts; it would control spacecraft operations; it would control tasking, balancing satellite tasking with other parts of the SIGINT system;

it would rid itself of the special NRO codewords, and would marry the SIGINT and overhead security systems, doing away with overhead compartments at NSA.<sup>50</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

~~(TS//SI//TK)~~ As an alternative to the expensive new system, some at NSA pushed an idea variously called "cheapsat" or "frugalsat." The idea which had been around for years, revolved around the need to support U.S. military operations. Most of the emitters in use

25X1

25X1

It would be far simpler to support military operations with a small, cheap satellite dedicated to mobile multichannel communications. In the mid-1980s the idea acquired a good deal of thrust when NSA discovered communications

25X1

25X1

in the low VHF range. Once again the idea of an "SMO satellite" bubbled up and got a thorough study within NSA. It never mustered enough support, and while NSA officially supported the concept, it was clearly a controversial item. Cheapsat always made the "options list," but it was never high enough up the queue to be funded.<sup>51</sup>

~~(TS//SI//TK)~~ The only part of the proposed system that NSA could call its own, absent a cataclysmic reorganization of the SIGINT overhead system, was processing. In the summer of 1986, NSA established a project to organize the ground processing system, called

25X1, 6

25X1, 6

would be very expensive

— a total of over \$957M. (see Table 27)<sup>52</sup>

~~(TS//SI//TK)~~ By mid-1987, NSA was becoming increasingly hostile to the new system as a solution. There were several reasons, any one of which might have led to a negative vote. First, cryptologic spending guidance from the DCI had begun to diverge from CCP guidance from the secretary of defense. This phenomenon had begun in 1983, and by 1987 the gap was some \$236 million per year and growing. Somehow it had to be closed, and overhead was a prime candidate. The new system would require huge expenditures for processing, first at 25X1, 6 and later at PL 86-36/50. Processing upgrade costs stood at about \$1 billion with the new system, but "only" \$600,000 without. This figure alone could close the gap or reduce it to a manageable size.

~~(TS//SI//TK)~~ Second, it was beginning to dawn on NSA that perhaps it was targeting the wrong sorts of signals. The new system was designed to intercept and process digital microwave signals, but the Soviets were not switching from analog to digital nearly as fast

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

(S//SI) Table 27  
 PL 86-36/50  
 USC 3605 Funding Profile<sup>53</sup>

FY 86	FY 87	FY 88	FY 89	FY 90	FY 91	FY 92
\$4.28M	12.35M	39.79M	208.M	265M	207.2M	219.75M

as had earlier been projected. As each year went by and the Soviets did not meet NSA's projections, the system looked more and more like a turkey.<sup>54</sup>

~~(TS//SI//TK)~~ In the fall of 1987, after a war of paper between NSA and the intelligence community staff, General William Odom took NSA's case to Congress. He had several complaints. NSA, he felt, could do everything with a more finely tuned 25X1 and 25X1 system than it could with a single new system, and spend less money at the same time. He criticized the new system for its lack of flexibility; with two systems NSA had a better chance to support military commanders, while with one system the capability to divert individual satellites to "hot spots" around the world would diminish. It was technically superior in ELINT, but less satisfactory in COMINT, which NSA felt was more important. And he did not like the vast sums required. "I thought [the new system] was sheer robbery of the public purse," he said later.<sup>55</sup>

~~(TS//SI//TK)~~ Much of NSA's dislike came down to system control. Odom felt that NSA's views had not been taken into account by NRO. He viewed NRO as a vast bureaucracy in which two programs, A and B, warred with each other, to the detriment of the national SIGINT manager. NRO tended to view the issue as a simple competition between a new program on the one hand, and two old programs 25X1 on the other. NSA looked at it in the context of the entire SIGINT system, and from that perspective a decision that seemed right to NRO looked wrong to NSA.<sup>56</sup>

~~(TS//SI//TK)~~ In January of 1988 the new DCI, Judge William Webster, cancelled the new system. In a letter to Senator David Boren of the SSCI, he explained that recent budget cuts put too much of a squeeze on the program. The NRO could save \$4.3 billion by not deploying it, and intended to do so. What he did not say was that NSA, the chief operator of the SIGINT system, was now in active opposition. But this was not news to Boren, owing to Odom's testimony on Capitol Hill.<sup>57</sup>

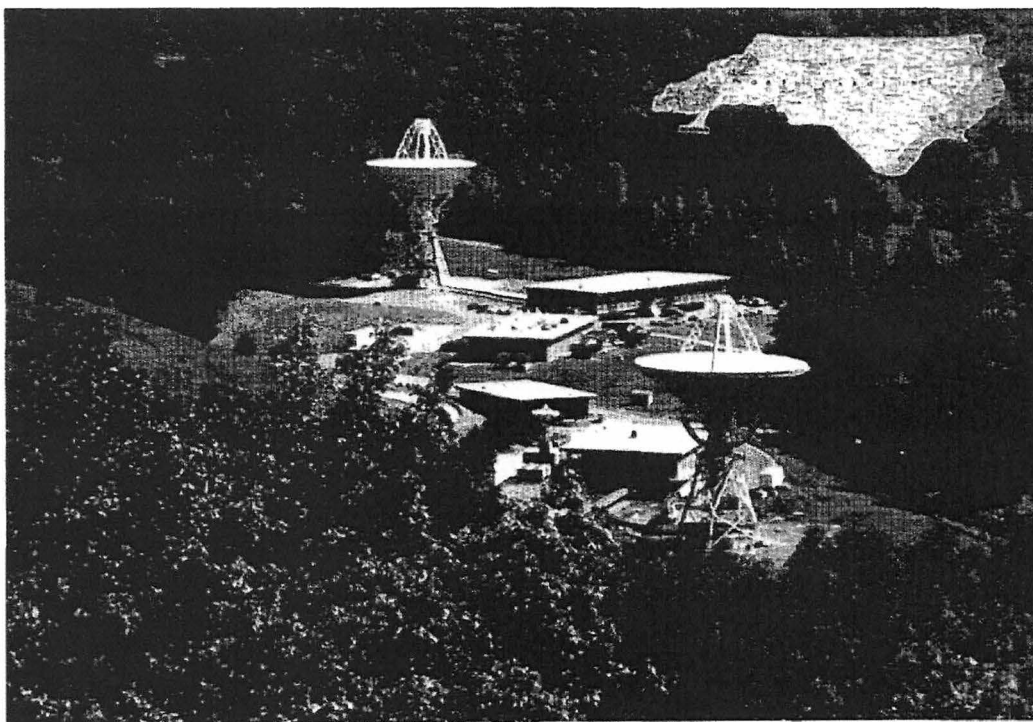
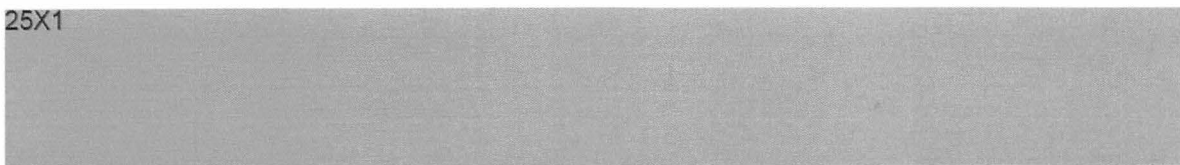
(U) Comsat

25X1


~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

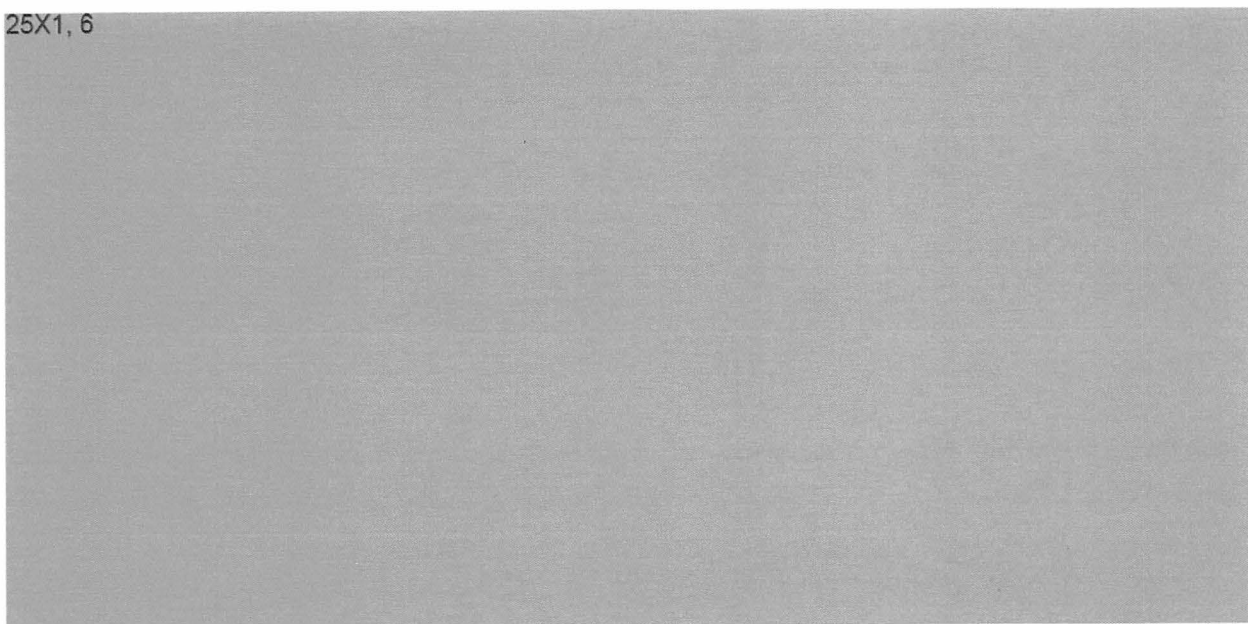
~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

25X1



(U) Rosman, North Carolina

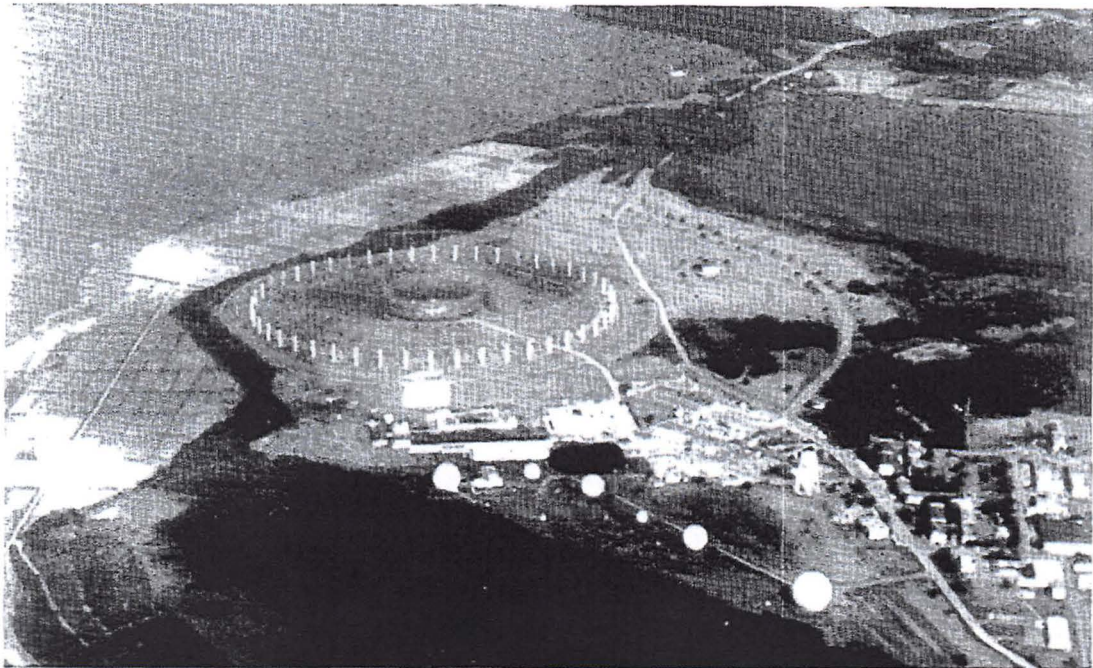
25X1, 6



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

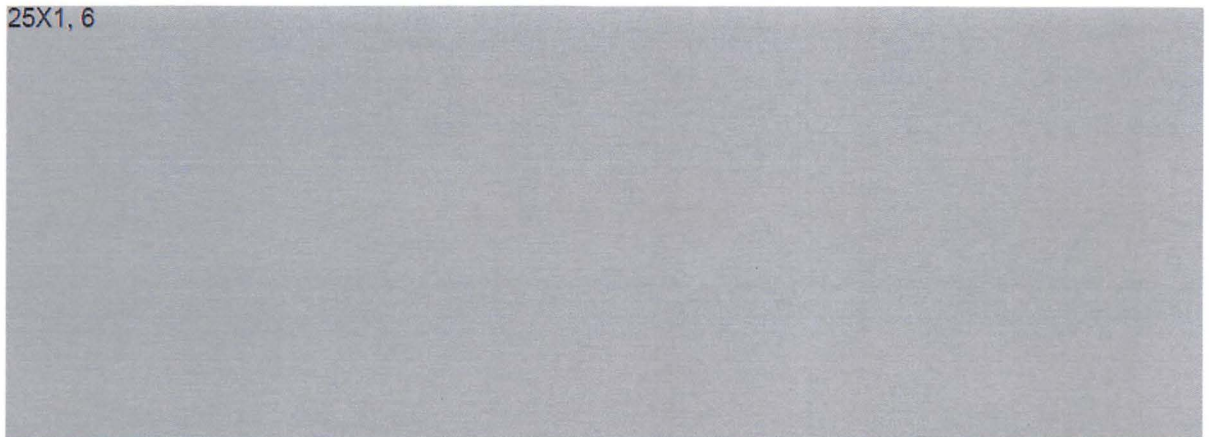


~~TOP SECRET//COMINT UMBRA/TALENT KEYHOLE//X1~~



(U) Misawa, Japan

25X1, 6



25X1



25X1

NSA's processing philosophy was to filter channels at the front end and return the cream to Fort Meade using high-speed communications. This demanded smaller, faster demodulators and demultiplexers, and

~~TOP SECRET//COMINT UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

high-speed communications packages. A whole range of equipment was specially designed PL 86-36/50 by NSA engineers. When, in 1984, NSA selected the IBM PC XT as its standard terminal, PL 86-36/50 USC 3605 also adopted it. Not only did the XT cost about one-fourth as much as the terminal it replaced, the Teletype Mod 40, but it matched up perfectly with the equipment in use at Fort Meade. In effect PL 86-36/50 USC 3605 underwent the same revolution in technology that Third Parties did when NSA finally took over those arrangements. Common equipment and common procedures turned out to be much more efficient.<sup>62</sup>

~~(TS//SI)~~ When NSA took over 25X1  
in 1978, the Agency found an ESC team 25X1  
25X1

25X1 NSA had the good fortune to  
inherit the 25X1 and life was easier as a result.

25X1

~~(TS//SI)~~ The cumulative improvements led to boom times PL 86-36/50 USC 3605 From 1979 to 1986  
PL 86-36/50 USC 3605 In 1979 PL 86-36/50 USC 3605 contributing to about 18  
percent of NSA product reports, while in 1986 the figure was 34 percent. This was  
achieved even though PL 86-36/50 USC 3605 and 5 percent of the  
Consolidated Cryptologic Program (CCP).<sup>64</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~**(U) Cryptologic Communications**

~~(C)~~ No area of cryptologic operations was expanding faster than communications. A chart of communications capacity from 1973 to 1993 (Table 28), first printed in the *Quarterly Management Review* for second quarter of 1994, depicted almost unbelievable numbers. Most dramatic was the worldwide capacity, which had increased by about 1,000 percent. Yet the system was being operated by about the same number of people as it had required twenty years earlier.

~~(S//SI)~~ Table 28  
Cryptologic Communications, 1973-1993

	1973	1993
Worldwide capacity	3 MBS	300 MBS
Number of circuits	746	5500
Messages annually	130,000	117 million
Secure phone systems	20 locations	150 locations
Instruments	11 thousand	34 thousand
Cost of communications	2% of CCP	5.5% of CCP
Manpower	1091	PL 86-36/50 USC 3605

(U//FOUO) NSA had become the largest single user of the DSSCS system, and by the early 1980s had outrun the ability of the DoD system to support it. The only answer was to lease large numbers of commercial circuits, from landline and microwave to satellite.<sup>65</sup>

(U//FOUO) Internally, NSA replaced its communications terminal system under a new project called EMBROIDERY. Under EMBROIDERY every communications terminal became a computer, just as field site collection positions were being computerized. Using off-the-shelf IBM equipment, NSA outfitted its Holder, IDDF/Underprop, OCEANFRONT, TIDE, TIDEWAY, and DAYSEND communications systems with new equipment and new methodology. TRAINMASTER, the field site portion of the system, replaced STREAMLINER, which had been deployed in the mid-1970s.<sup>66</sup>

(U) NSA's impressive communications design capability was sometimes employed in the service of other organizations. This was the case with a system called Umstead, a commercial design originally adapted for government use by an NSA engineer named PL 86-36/50 USC 3605 to transmit voice and data via satellite. It was light, mobile and inexpensive, and looked like the answer to an Army tactical communications problem. The Army's problem came into rather stark relief during a large 1981 exercise called Crested Eagle. Army tactical forces simply lacked enough communications channels to carry what they needed, and intelligence got such a low priority that little of it got to the

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

customers. Sixty percent of the signals intelligence traffic had to be couriered, and much of it was still in courier two weeks after the exercise had ended.

(U) Through mid-decade, top Army field commanders insisted that Umstead would solve the problem. But it was opposed by Signal Corps generals on somewhat obscure grounds, and was never purchased. Umstead was used on a few occasions by NSA, but never achieved its true potential, and wound up sitting on the shelf.<sup>67</sup>

#### **(U) Cryptologic Computers**

(U//FOUO) If the 1960s and 1970s were the era of mainframe computers, the 1980s were an era of small systems. By the late 1970s the mainframes at Fort Meade were becoming so congested that they looked like the Beltway at rush hour. As access time increased, a movement away from mainframes accelerated. In the early 1980s computer companies were beginning to produce personal computers in large quantities at low prices, and NSA managers began defecting to these systems. Kermit Speierman and Walter Deeley were early proponents of personal computers and off-the-shelf software.

(U//FOUO) The improved efficiency and cost effectiveness of the computer-on-every-desk approach was counterbalanced by a strong trend toward nonstandard equipment and software. With so many products available in stores, it was difficult for NSA's computer people to keep up. The driver was maintenance: when hardware and software malfunctioned, it was impossible to keep everything running. Moreover, central control over formats, file access, etc., the basis of the cryptologic system's effectiveness, could be lost. Chaos could be the result.<sup>68</sup>

(U//FOUO) To save the situation, NSA tried to standardize PC hardware. In 1984 it issued a request for proposal for an Agency Standard Terminal Workstation (ASTW). The IBM PC XT, a relatively new entry in the world of personal computers, won the award. It was a big win: the contract was ultimately valued at \$199 million, and NSA bought 21,000 units. The next year the Agency awarded a contract for an Agency Standard Host (ASH), which would interconnect the ASTWs. American Telephone and Telegraph won the contract, valued at \$150 million. Seven hundred twenty systems were finally sold to NSA.<sup>69</sup>

(U) In the early days, most personal computers ran on the DOS operating system, but it was not suitable for internettted systems. Kermit Speierman of NSA discovered that Bell Laboratories had devised an operating system called UNIX, which was at the time the only system that operated in a multi-user, internettted environment. UNIX became the dominant operating system in the 1980s.<sup>70</sup>

(U//FOUO) Computer power was the essential ingredient in cryptanalysis. In the 1970s NSA had forged ahead with the help of supercomputers, first from Control Data Corporation (CDC) and later from Cray. But the early 1980s were a period of tension in the supercomputer business. The Japanese were rumored to be about to enter the business, and in view of their devastating impact on the commercial VCR business, there

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

was a potential threat to national security if American supercomputer companies were to be bested or even driven out of business. These problems were part of the background noise of 1982, when NSA's Kermit Speierman was doing some work at Los Alamos and talking to scientists there about NSA's computer power problems. The outgrowth of those discussions was a decision to jointly host a conference at NSA in 1983 on supercomputer problems. Called "Frontiers in Supercomputing," the week-long conference focused on how to design and build faster supercomputers. It was clear that serial processing would not be fast enough – the industry needed massively parallel processing to have a chance of staying ahead.<sup>71</sup>

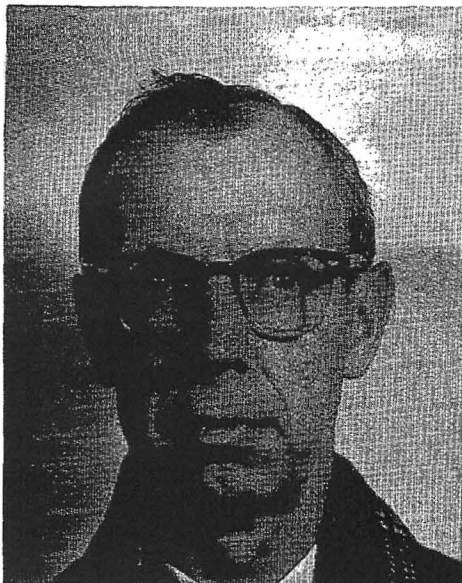
(U//FOUO) General Faurer, who gave the closing speech, had become convinced that a permanent institute was needed, and asked Speierman to create one. Working through an NSA committee, Speierman put together a concept for a Supercomputer Research Center. Faurer needed \$16 million and a lot of executive push, so he briefed the outlines of the research center around Washington. He was able to muster support from every quarter but the JCS and the Office of the Secretary of Defense, where his boss, William Taft, was staunchly opposed. But Taft was ultimately outflanked, and NSA began looking for a home for the center. Although Boston and North Carolina were considered, NSA finally selected the nearby Bowie area, and on November 27, 1984, Maryland governor Harry Hughes announced from the steps of the State House in Annapolis the creation of the Supercomputer Research Center.<sup>72</sup> The center would not have survived without Faurer's forceful intervention at the DoD level. Said Speierman several years later, "...he was completely convinced. I think that's a real tribute to him. And he never flinched from that conviction. Without that 100 percent conviction on his part...I don't think any of this would have happened."<sup>73</sup> It was one of the disputes with Taft that resulted in Faurer's early departure from NSA.

#### **(U) Computer Security**

(U) In 1965 a small computer science firm called SDC of Santa Monica, California, became concerned about security of their computer products. With computer networking in the offing, computer files could become vulnerable to unauthorized users, almost as if a safe had been jimmied. SDC hosted a conference attended by several computer companies and by the head of the Rand Corporation computer sciences division, Dr. Willis Ware. Ware quickly took the lead on the issue.<sup>74</sup>

(U//FOUO) Ware, as it happened, sat on NSA's Scientific Advisory Board, and called General Carter to tell him that he was about to get a hot new issue on his plate. Contending that NSA was the only agency in the federal government that had the technical expertise, Ware plugged for the Agency's direct involvement. The issue bubbled slowly for two years, but in 1967 the Defense Supply Agency (DSA) at Cameron Station, Virginia, made a formal request to the secretary of defense that NSA be named the computer security authority. This was followed in short order by requests from several other federal agencies. NSA first became involved with these requests on a voluntary basis – it had no charter to do this unless cryptographic equipment was involved, and

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

(U) Dr. Willis Ware

in this case it wasn't. Nor did NSA have an organization officially tasked with the job. The DSA request to the secretary was still pending and had generated a lot of controversy within NSA. Many felt that NSA should avoid the task.

(U//FOUO) Having dodged responsibility for the new COMPUSEC mission for several years, NSA finally made a partial step in 1969 with the issuance of a memorandum by the deputy director, Louis Tordella. Noting that NSA possessed no official responsibility, Tordella nonetheless acknowledged that a moral responsibility was involved. Thenceforth, NSA would provide assistance to other intelligence community (IC) organizations based on experiences that NSA had had with its own systems. NSA would not assist non-IC organizations.<sup>75</sup>

(C) In 1972, the consequences of continued inaction were starkly illustrated by an incident involving DIA. The Defense Intelligence Agency had created several intelligence community databases designed for multilevel security access, and DIA contacted USIB about running a security check of the system so that they could get their systems accredited for SI and TK information. NSA and other members of the intelligence community, with participation from defense contractors, obliged. By the time the attacks terminated, the penetration was so thorough that a penetrator at a distant remote terminal had actually seized control of the system. DIA never got its accreditation, and the results of the exercise made many at NSA skeptical that multilevel security could ever be achieved.

(U//FOUO) NSA's role in computer security expanded in 1973. Needing a focus for research on the subject, Tordella named the ADC (assistant director for comsec) as the responsible official, and ADC established a small center for technical information on the subject, specifically to support federal agencies. Despite Tordella's decision, however, little happened through the end of the decade. Lew Allen requested sixty-seven billets for the fiscal year 1975 program, but was turned down, in part because NSA's role was still controversial.<sup>76</sup>

(U//FOUO) Late in the decade an OSD staffer and former NSA employee, Stephen Walker, approached Bobby Inman about the computer security mess. Walker explained that in OSD there was a strong feeling that NSA should expand its effort and become the office of primary responsibility for computer security in the federal government. However, Walker personally opposed locating the organization within COMSEC. Inman agreed and asked George Cotter, the assistant director for telecommunications, to take on the task.

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

Working closely with Walker, Cotter set up the Computer Security Center as a separate organization. It was formally created on the first of January, 1981, as the Department of Defense Computer Security Center, with a small staff working directly for Cotter. Originally it was to have a separate building, to be located in the parking lot outside Ops-3 on the main Fort Meade campus. But, as often happens with money, the line item was diverted, and went into construction of the Special Processing Laboratory. In the end, the center never got its own building, and it continued to operate out of borrowed spaces.<sup>77</sup>

(U//FOUO) NSA's role in computer security remained a lightning rod for dissent both within NSA and in the outside world. That role waxed and waned depending on the political winds. Under Reagan, it expanded, and under NSDD 145 the DoD Computer Security Center became the National Computer Security Center, with an expanded mission to bring computer security products to non-national security organizations. At the same time, Walter Deeley and Harry Daniels, who were running the COMSEC organization, convinced General Odom that COMPUSEC should be part of their organization, and so the Center was resubordinated to the (now called) DDI, responsible for INFOSEC, which included both COMSEC and COMPUSEC.<sup>78</sup>

(U) But NSDD 145 encountered congressional opposition, and it was overturned in 1987 by the Computer Security Act. This legislation split the mission between NSA and the National Bureau of Standards (NBS, which soon changed its name to NIST, National Institute of Standards and Technology). NSA retained its role within the national security community, but NBS got the mission to deal with all others. It was clear from the legislation, however, that NSA would retain a strong technical advisory role with NBS, which lacked the expertise on the subject.<sup>79</sup>

#### **(U) Operations Security**

(U) The experience in Vietnam had generated an operations security program called Purple Dragon (see Vol II, 551). NSA had been the core of the effort, and it became the institutional memory for OPSEC. But as Vietnam faded from mind, memories of OPSEC programs grew dim. So in the early 1980s NSA began holding OPSEC seminars around the Pacific Rim for military organizations. The program quickly expanded to the Coast Guard, the White House, GSA, Customs, and NASA. This nascent effort became a full-blown OPSEC training program at the National Cryptologic School. The National OPSEC Course was open to all federal agencies, and 80 percent of the attendees were non-NSA.<sup>80</sup>

~~(C)~~ In 1983 Caspar Weinberger directed that all DoD organizations have OPSEC programs, and NSA became responsible for OPSEC education. But while NSA spread the word about effective OPSEC programs, it had none itself. The "Year of the Spy" (see page 401) brought on a thorough internal examination of security practices. The panel, headed by David Boak concluded in 1986 that NSA had effectively flunked its own OPSEC exam. This led to the establishment of a DDI OPSEC working group to bring NSA into compliance with its own established standards.<sup>81</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

(U) In 1988, President Reagan signed NSDD 298, which established the OPSEC program of the federal government. Every agency with "classified or sensitive activities" would establish a formal OPSEC program. The order gave NSA the training and technical support mission for all federal programs. It also established an Interagency OPSEC Support Staff, with representatives from NSA, FBI, CIA, DOE, and GSA. A SIGINT professional, Carl Miller, was named to head the NSA effort.<sup>82</sup>

**(U) INFOSEC and the New Way of Doing Business**

~~(C)~~ In 1983 the Communications Security organization got a new boss. Walter Deeley, who had revolutionized SIGINT timely reporting, was sent by General Faurer to do the same thing to the COMSEC business. Deeley took stock of American COMSEC, and did not like what he saw. As he later said to a congressional committee, "I was appalled. Within weeks I told Faurer that I would rank the United States in the top half of the Third World countries when it comes to protecting its communications. What I found was a secluded organization with fewer than 2,000 people, including all the printers of our codes and ciphers, no charter to effect change, no money except to engage in research and development, and customers who really didn't want our products."<sup>83</sup> Two years later he said to another committee: "The United States is in jeopardy because it does poorly protecting its vital communications....As a nation so far, we have not made this commitment...."<sup>84</sup>

(U) The New Way of Doing Business, as the Deeley revolution was termed, was based on embeddable COMSEC products, or "COMSEC on a chip." Instead of protecting point-to-point circuits, NSA would go for bulk encryption. The Agency would get into a partnership with commercial manufacturers to produce encryption technology. The revolution did not just happen; it was carefully planned and executed.<sup>85</sup>

(U//FOUO) One of the first battles of the Deeley era was over national policy. The struggles of the Carter administration over what federal agency was to control national COMSEC policy continued into the Reagan years. Admiral Bobby Inman had been sure that Carter would lean toward expanded authorities by the Department of Commerce, and he successfully stalled the Carter White House on the issue, hoping for a more favorable decision from the incoming Reagan people.

~~(C)~~ The new administration was temperamentally inclined to give the problem to DoD. This was strongly reinforced by the problems in Soviet exploitation of U.S. domestic communications, the problems with Moscow embassy security, exposure of the Walker ring, and concern over potential penetration of American computer systems. A coterie of NSC staffers, headed by Kenneth deGraffenreid, pushed hard for NSA involvement. The result was a new National Security Decision Directive, NSDD 145. Issued in 1984, it established COMSEC as a high-priority national objective, and named the secretary of defense as the executive agent for the security of government communications related to national security. NSA was designated the "National Manager for Telecommunications Security and Automated Information Systems Security," a longish title which placed the

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

Agency directly in the center of the COMSEC business. Moreover, NSDD 145 did away with the old United States Communications Security Board, which had accomplished so little over the years. Instead, the directive replaced it with a new Systems Security Working Group (SSSC) and, under it, the National Telecommunications Information Systems Security Committee (NTISSC, pronounced "entissic"). NBS had separate responsibility for the private sector, but even there, NSA had a technical and advisory role. NTISSC, the real player in this game, was dominated by NSA, and its secretariat was located in NSA spaces.<sup>86</sup>

(U) The ink on NSDD 145 was hardly dry when it was attacked in Congress. The issue turned on a congressional distrust of DoD involvement in computer security. The Department of Commerce, which had been involved in COMPUSEC by the Carter order (PD 24), was anxious to reverse the course of NSDD 145, and a behind-the-scenes brawl developed between NSA and Commerce over the COMPUSEC authority. The fight was ultimately settled by Congress, which in 1987 passed Public Law 200-135, legislation which was promoted by Congressman Jack Brooks of Texas. This gave Commerce control over COMPUSEC in all cases except those involving classified government contracts, in which NSA was still the prime actor. Although the new law was supposed to affect only computer security, NIST was expected to establish crypto standards and policy for computer security, a domain in which NSA had formerly operated with complete freedom. The hearings which led to the legislation revealed the huge technological lead that NSA enjoyed in the field of computer security, but the demons of congressional distrust could not be overcome.<sup>87</sup>

~~(S)~~ The secure voice revolution that had begun in the 1970s accelerated under Deeley. He brought with him the perspective of a SIGINTer who knew how to exploit other countries' communications.

...twenty years ago I was...having fun listening to Khrushchev and Ustinov and all of them riding around Moscow talking their heads off in their sedans....When I walked into this [job] two years ago, the president and cabinet members and the chairman of the Joint Chiefs of Staff and every other dignitary of government were riding around in their sedans blowing every secret we have over clear telephones - 18 years later we were still doing that.

~~(TS)~~ By the time he took over, the formerly simple picture had been complicated by the Bell Systems divestiture, mandated by a federal government antitrust suit. This forced NSA to deal with many firms to secure wirelines, instead of just one or two. PL 86-36/50 USC 3605  
PL 86-36/50 USC 3605  
PL 86-36/50 USC 3605

what was needed was a truly user-friendly secure voice handset. In 1980 Deputy Secretary of Defense Graham Claytor endorsed the STU-II program and recommended large-scale procurement. In 1982, his successor, Frank Carlucci, decided to buy 5,000 STU-II sets and allocated \$120 million for the program. The STU-II was strongly endorsed by Alexander Haig, Carlucci and President Reagan himself.<sup>88</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~(S)~~ But STU-II was just a waystation. The revolution in voice security was wrought by a new product, the STU-III. The basis for the STU-III was a public key algorithm called Firefly, designed by engineers from NSA's R1. When Deeley came to the COMSEC organization, he "captured" R1 and created a special projects office to develop the STU-III. Deeley made the decision to have the STU-III built by private industry, and three contractors - RCA, AT&T, and Motorola - each developed a unique STU-III device, all three of which sold competitively. It was a low-cost (about \$2,000 per copy) terminal that would sit on a desk. There would be unique plastic key for each device, but the device would not work without another key, developed on demand from a central key management center. The Key Management Center would re-key each device at least once a year. The key generation system relied on an algorithm that would find large prime numbers very quickly. <sup>25X1</sup>

25X1

(U) The key management facility was originally collocated with a contractor in Waltham, Massachusetts. In 1988 NSA moved the facility to an old 1950s-era bomb shelter in the Maryland countryside owned by AT&T, near Finksburg.<sup>90</sup>

(U) The crypto gear that NSA had designed for the new communications era had, by the early 1980s, come to the end of the rope. The KW-26, a marvel of its day, could only secure 100-word-per-minute circuits. The KG-13 and KW-7 were out of production and becoming more difficult to maintain every day. The replacement device, developed under a project named Yellowfin, would be the KG-84. Small, lightweight (20 lbs), cheap (base price of about \$5,100), it was designed to operate at speeds up to 9600 bps. Cost of maintenance was also a big selling point: while the KW-26 mean time between failure (MTBF) was 1,840 hours, the worst-case MTBF for the KG-84 was 17,000 hours. The KG-84 began appearing in comm centers in the mid-1980s.<sup>91</sup>

~~(C)~~ One of the COMSEC improvements of the 1980s was OTAR (over-the-air re-keying). NSA had long wanted to dispense with paper tape re-keying, with its attendant courier problems and possibility of loss or pilferage. The Agency had incorporated OTAR into the Vinson tactical voice system of the late 1970s, but the rationale was combat. If an American unit with a Vinson were overrun, the field commander would need a way to quickly re-key all other Vinson equipments. Vinson was an OTAR device by exception only; it was normally keyed just like any other COMSEC device. The KG-84 was designed with an optional OTAR capability, but DCA thought so little about it that at one time it directed that all KG-84s be rewired to disable the OTAR feature.<sup>92</sup>

~~(C)~~ But two events in the 1980s spurred a reversal of fortunes for the OTAR concept. One was the invasion of Grenada, which conclusively demonstrated that the services could not easily talk to each other, and drove the JCS to reform the concept of jointness and to direct the services to marry their communications system. This led, ultimately, to a new COMSEC key distribution doctrine which would permit U.S. forces to communicate with each other on almost all tactical crypto devices using electronically distributed key.<sup>93</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA//TALENT KEYHOLE//X1~~

(U) The second was the arrest of John Walker in May of 1985 (see page 417). Walker had been stealing crypto key since 1968 and selling it to the Soviets. The massive hemorrhage of classified information was directly attributable to the wide and easy availability of crypto key, and sparked a complete re-look at COMSEC keying doctrine.

~~(S)~~ What resulted was a JCS decision in 1988 to implement OTAR on every KG-84 device in the world. Vice Admiral Jerry Tuttle, the JCS J6 in 1988, forced the issue after being told that NSA was having a hard time keeping up with the demand for paper keying tape and that the KG-84 had been designed with an OTAR capability that was not being used. Tuttle made the historic decision to require OTAR on KG-84 circuits, and by the early 1990s the KG-84 had been completely converted to the new method of operation.<sup>94</sup>

(U//FOUO) Until NSA came up with an effective OTAR strategy in the 1980s, the best it could do was to protect the crypto keys from tampering. The Agency always had a small group working on protective packaging, but the big breakthrough came with the hiring of a chemist named PL 86-36/50 USC in the 1960s. PL 86-36/50 a Harvard Ph.D. in chemistry, had specialized in the detection of poison gasses during World War II. After the war he worked for CIA on protective packaging until he switched to NSA. He brought with him the techniques of the spy.<sup>95</sup>

~~(S)~~ PL 86-36/50 introduced many new packaging techniques. For key tapes, NSA developed 25X1

25X1

25X1

25X1 John Walker said in his debriefing that he tried to steal key that was canister protected, but gave up and just stole key that was easier to pilfer. This lent a huge push for canister protection.<sup>96</sup>

~~(S)~~ For key cards and authenticators, PL 86-36/50 and his group developed methods to 25X1

~~TOP SECRET//COMINT-UMBRA//TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~(S)~~ But occasionally the game became real. In 1982 the COMSEC threat analysis group under Dr. William Ward sent 300 bogus specially packaged one-time pads to users throughout the world. (They were bogus in the sense that they were not to be used; they were to be returned without opening by the recipient.) Back at NSA, the packages were subjected to laboratory analysis to see if they had been tampered with. Two hundred ninety-nine came back clean. One package - the one addressed to PL 86-36/50 USC 3605 - had been opened.

PL 86-36/50 USC

3605

25X1

~~(S)~~ Ultimately the penetration operation was halted. But for PL 86-36/50 USC 3605 packaging and the "dangle" operation mounted by Ward, the Polish intelligence service could have continued stealing crypto key indefinitely.<sup>99</sup>

#### **(U) The Second Parties - the United Kingdom**

~~(S//SI)~~ Relations with the British, relatively sunny even in the worst of times, enjoyed "gold star" status after the Falklands War (see page 374). In this case, the Reagan administration made a commitment, though somewhat tardy, to throw its support behind the British.<sup>25X6</sup>

25X6

It was probably the high point for the relationship since World War II.

(U//FOUO) In the mid-1980s, CIA headed a study of America's close intelligence relationships. The subcommittee on the U.K. relationship, reporting in January of 1988, began with the statement that "No country has closer or more extensive diplomatic and intelligence liaison ties to the United States than does the United Kingdom. The 'special relationship' between the two governments on intelligence matters has existed since the outbreak of World War II."

~~(S//SI)~~ Although calling the CIA-U.K. relationship the broadest in terms of scope, the committee characterized the NSA-GCHQ liaison as the most fully integrated. It concluded that it would be more accurate to call it an "equal partnership" than an exchange of information. NSA assessed that this was likely to become more rather than less

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

integrated, pointing to total integration of British and Americans at 25X1, 6 sites, fuller exchanges on the international terrorism target, the need to broaden access to 25X1, 6 signals through 25X1, 6 and plans for a multinational effort to recoup the Hong Kong collection following British pullout from the Crown Colony in 1997.<sup>100</sup>

(S) The only serious rift was on the COMSEC side. Relationships in that area had never been as strong as on the SIGINT side. In 1986, when the STU-III was still under development, NSA decided not to exchange with foreign partners, excepting only Canada (to service the needs of the NORAD joint strategic defense effort). The decision was based on reluctance to release to foreign countries the Firefly key management system. NSA devised a work-around that involved releasing the STU-II to NATO nations, and developing a modification, called STU-IIB, which would permit interoperability with a modification of STU-III. The STU-III variant could talk with other STU-IIIs, but the original STU-III could not talk with STU-IIBs. It was a convoluted system, but the DDI organization insisted that it would work.

(S) Although NSA held to the original decision, it resulted in high-level complaints from GCHQ. How, it was asked, could NSA justify bringing Canada into the system, but not the British, with whom there was a much closer cryptologic relationship? Moreover, the decision was hardly unanimous within the U.S. Admiral Jerry Tuttle, the JCS J6, surfaced the issue in 1988. This occasioned a note from NSA's foreign relations directorate that the NSA position "makes arguments that are illogical, weak, and indefensible." Dissent notwithstanding, the NSA position did not waver.<sup>101</sup>

(TS//SI) One of the most influential SIGINT joint partnerships was a mysterious project called 25X1, 6. The partnership between NSA and GCHQ 25X1, 6 brought GCHQ into an indirect association with 25X1, 6. It raised some very good questions about the viability of continued reliance on 25X1, 6 and GCHQ senior managers began turning the question over in their minds. GCHQ informally approached Director Lew Allen through the NSA representative in London, Milton Zaslow, in 1976. 25X1, 6

25X1, 6 but Allen felt strongly that this would fragment the British SIGINT effort and 25X1, 6

25X1, 6 However, GCHQ persisted and brought matters to a head at a 1979 joint NSA-GCHQ conference. 25X1, 6

25X1, 6

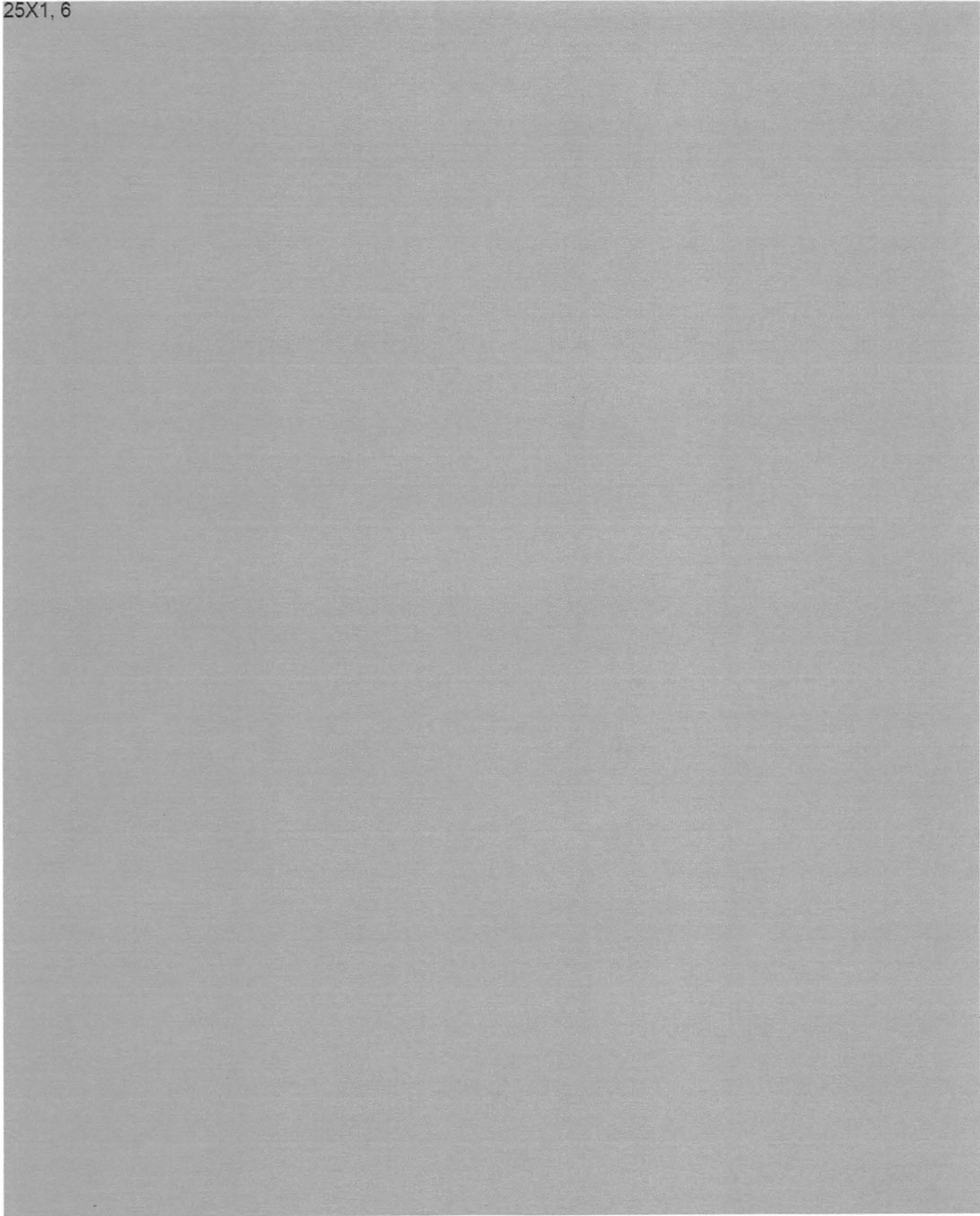
25X1, 6

By 1979, Admiral Bobby Inman was the director, and the GCHQ proposal fell on more sympathetic ears.<sup>102</sup>

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

25X1, 6



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~**(U) Australia**

~~(S//SI)~~ Despite the bumpy times of the 1970s, the relationship with Australia enjoyed an unprecedented expansion during the following decade. In the late 1970s DSD had committed to a major joint project, <sup>25X6</sup>

25X6

25X6

and with considerable help from NSA technical people, and an on-going partnership with GCHQ, Australia got into <sup>25X6</sup>

25X6

~~(S//SI)~~ <sup>25X1, 6</sup> was followed soon after by an even larger project. <sup>25X1, 6</sup>

25X1, 6

25X1, 6

Despite the heavy capital expenditures that would be involved, and the huge management problems that would inevitably ensue, <sup>25X1, 6</sup>

25X1, 6

(U) Australia's parliament had been controlled by Conservatives since the sacking of Gough Whitlam in 1975. But in 1983 the Australian Labor Party (ALP) regained control. The left wing of the party had been critical of Prime Minister Malcolm Fraser's close relationship with the United States. There were threats to close Aussie ports to American warships and strident declarations of brotherhood with the government of Vietnam. But when party leader Bob Hawke took the premiership, he excluded the left wing of the party and repudiated the anti-U.S. planks of the party platform. In foreign affairs he formed a close bond with Ronald Reagan. Soon after his election he publicly declared that the U.S. would continue to enjoy access to defence facilities in Australia, including Alice Springs (also known as Pine Gap). His public statement in support of the facility revealed the base's purpose: "...provision of early warning by receiving from space satellites information about missile launches - and the occurrence of nuclear explosions." It was more than the U.S. wanted him to say, but was received with relatively good graces in view of his strong support for the joint effort.<sup>106</sup>

25X1, 6

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



(U) Bob Hawke, second from left

25X1, 6

(U) *New Zealand*

~~(S//SI)~~ The fifth UKUSA partner was New Zealand. Since World War II, New Zealand had maintained a cryptologic relationship with the Commonwealth countries and the United States through Australia. This subterranean channel changed in 1980, when New

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

Zealand forged a completely independent relationship between its cryptologic organization, GCSB, and NSA. A New Zealander was assigned as liaison to NSA, and later in the decade NSA sent a representative on a PCS tour to GCSB to assist the host country to plan and organize its cryptologic effort.<sup>108</sup>

(U) The new relationship occurred just in time for controversy. In the summer of 1984 the Labor Party under David Lange assumed power in New Zealand. The party had long had a nuclear-free plank, and left-wing members were pressing for withdrawal from ANZUS. Lange, being a centrist by persuasion, tried to ignore the anti-U.S. tide, continuing to push a decision into the future. The Reagan administration also tried to ride out the storm, believing that Lange would be a New Zealand Bob Hawke on the issue. But it did not understand the depth of Lange's difficulties. Lange's problem turned on the nuclear-free issue and the determination of his left wing that no American nuclear vessels would be permitted in New Zealand ports. The U.S. delayed port visits in hopes that Lange could solve the political problem. Finally, in March of 1985 the U.S. requested permission for a non-nuclear vessel, the USS *Buchanan*, to visit Auckland in connection with a scheduled naval exercise. This was done under a tacit agreement with the Lange government that the first port visit would be by an obviously non-nuclear vessel, following which Lange could announce that he had determined that it was not a nuclear vessel and could enter. But the deal broke down because Lange could not push it through his party caucus, and he announced that the *Buchanan* would not be permitted to enter port. The outraged Reagan administration cancelled the joint exercise and suspended all military cooperation with New Zealand, including the flow of intelligence information.<sup>109</sup>

~~(S//SI)~~ Fortunately for NSA, cryptology was one of the few exempt areas. Relationships continued, albeit at a somewhat reduced level. By 1989 relations had improved to the point that NSA assisted GCSB to set up <sup>25X1, 6</sup> collection facility. The permission was granted because the agreement had predated the 1985 nuclear ship fiasco.<sup>110</sup>

#### (U) Third Parties

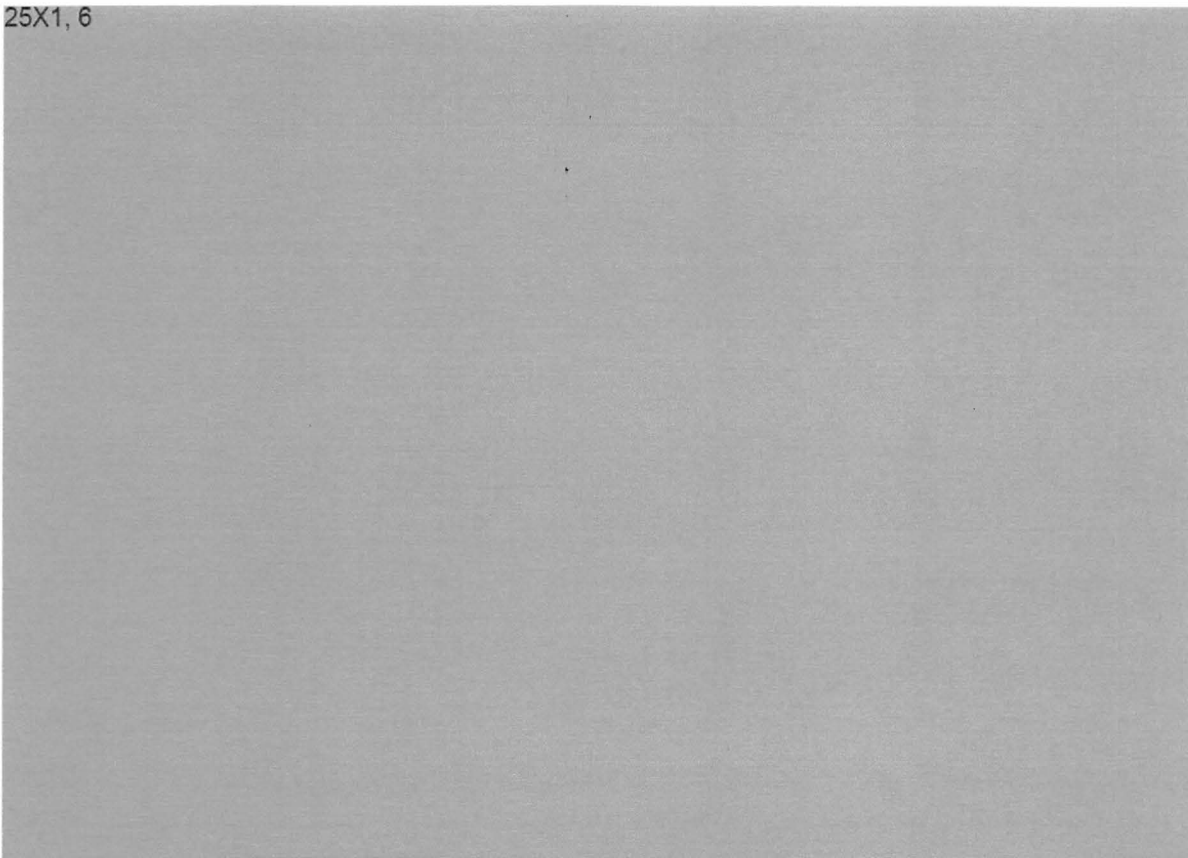
~~(TS//SI)~~ The 1977 Peace Treaty with CIA behind it, NSA devoted the 1980s to the process of cementing its technical exchanges with Third Parties. As the importance of Third Parties increased, relations inevitably expanded, and in the early 1980s NSA and GCHQ were confronted with difficult technical exchange questions. <sup>25X1, 6</sup>

25X1, 6


~~TOP SECRET//COMINT//UMBRA//TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

25X1, 6



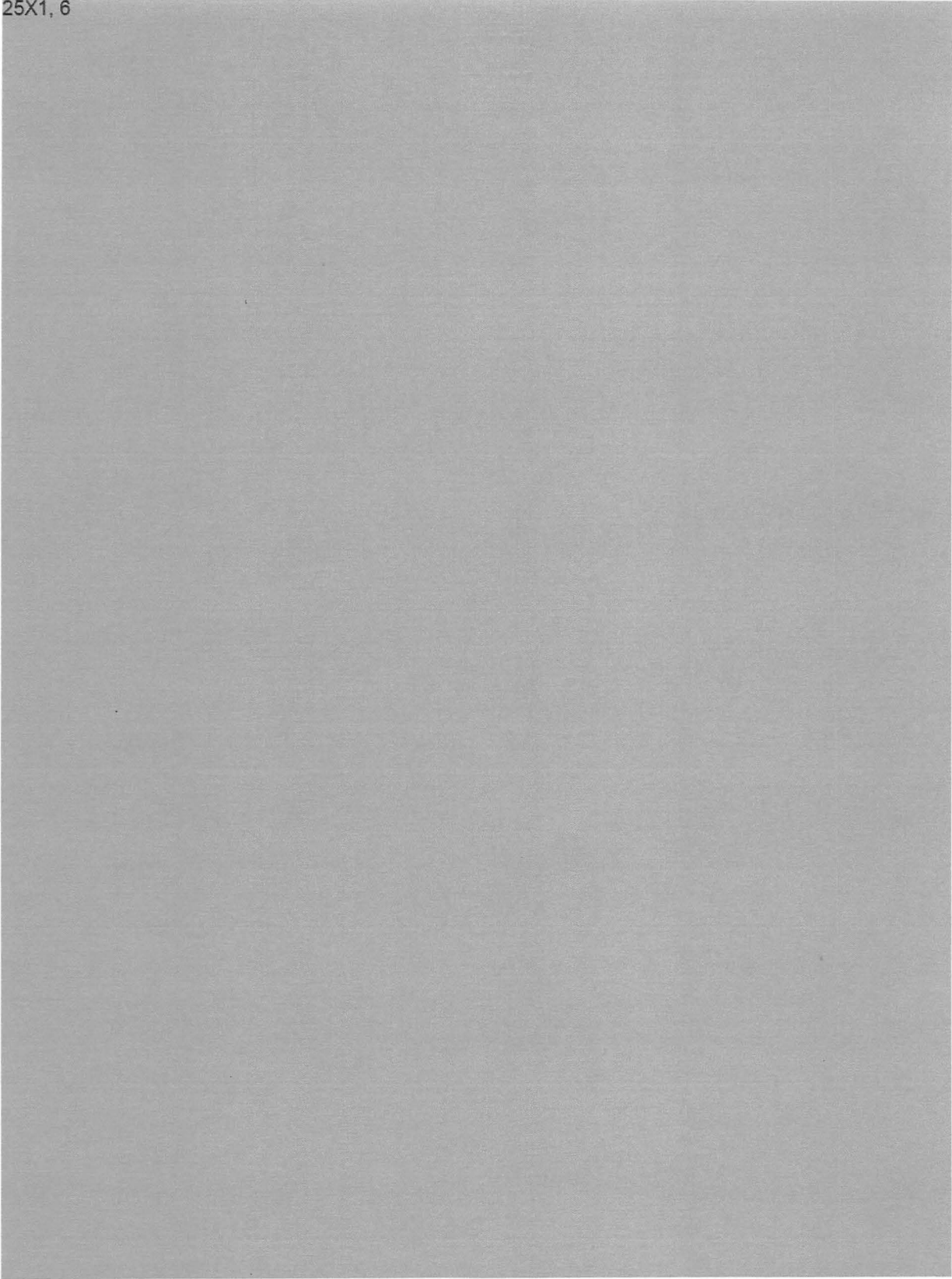
~~(S//SI)~~ Foreign relationships had always been bilateral, in accord with UKUSA principles. Thirty-five years after the accords, however, the principle was beginning to fray. 25X1, 6



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

25X1, 6

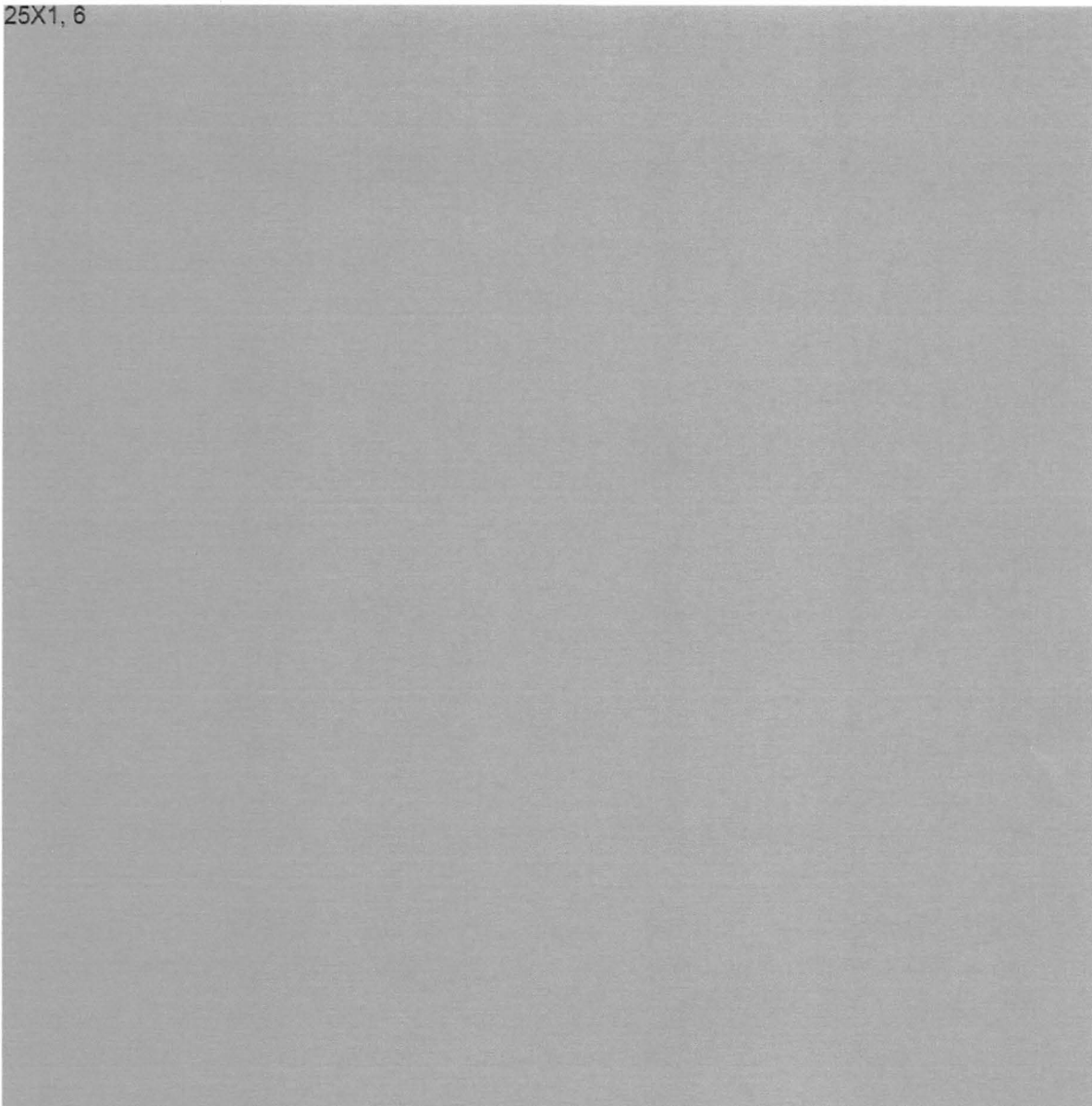


~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~



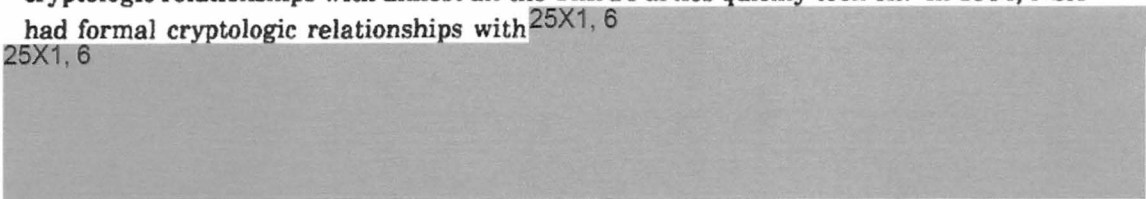
~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~

25X1, 6



**(U) All The Rest**

~~(TS//SI)~~ Once freed from the restrictive CIA direct oversight of Third Party operations, cryptologic relationships with almost all the Third Parties quickly took off. In 1984, NSA had formal cryptologic relationships with <sup>25X1, 6</sup>  
25X1, 6



~~TOP SECRET//COMINT-UMBRA/TALENT KEYHOLE//X1~~