National Security Agency

Defending Our Nation. Securing The Future

National Security Agency

60 Years of Defending Our Nation

National Security Agency, circa 1950s.

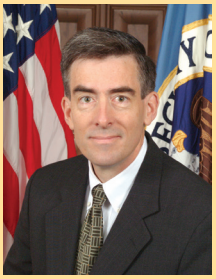
On November 4, 2012, the National Security Agency (NSA) celebrates its 60th anniversary of providing critical information to U.S. decisionmakers and Armed Forces personnel in defense of our Nation. NSA has evolved from a staff of approximately 7,600 military and civilian employees housed in 1952 in a vacated school in Arlington, VA, into a workforce of more than 30,000 demographically diverse men and women located at NSA headquarters in Ft. Meade, MD, in four national Cryptologic Centers, and at sites throughout the world.

While the mission to defend the Nation against all adversaries has not changed, the adversaries have changed considerably. During the Cold War, NSA's primary focus was on the Soviet challenge, punctuated by tense crises, such as the one in Cuba in 1962. After the breakup of the Soviet Union, the adversary was less likely to be wearing the uniform of a specific country. In fact, today our greatest threat may be a lone person using a computer.

Throughout its six decades, NSA has pursued its mission by employing smart, committed, and courageous people, developing innovative technology, partnering with allied nations, and collaborating with our DoD and IC colleagues. Our commitment to upholding the law of the Nation and protecting the civil liberties of its people has never wavered.

On behalf of the dedicated employees of the National Security Agency, we are pleased to present this publication that tells the fascinating story of NSA – 60 years of "Defending Our Nation and Securing The Future." We have only just begun.

KEITH B. ALEXANDER
General, U.S. Army
Director, NSA/Chief, CSS



John C. Inglis
Deputy Director
National Secuirity Agency

THE WHITE HOUSE

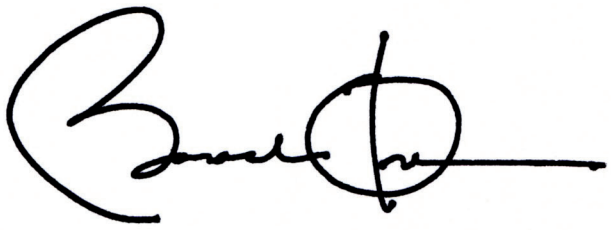
WASHINGTON

August 31, 2012

I am pleased to congratulate the National Security Agency (NSA) on its 60th anniversary.

Since its inception in 1952, NSA has played an essential role in protecting our Nation from those who would do us harm. From the Cold War through modern conflicts across the globe, the agency has been at the forefront of securing our communications, defending our networks, strengthening our insight into global affairs, and supporting our Armed Forces. As the civilian and military personnel of NSA reflect on six decades of service, I trust you take great pride in the work you do each day to keep America safe.

Congratulations, again, on this special milestone. I wish you all the best for the years ahead.



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JUL 17 2012

General Keith B. Alexander, USA
Director, National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6242

Dear General Alexander:

I want to extend my congratulations on the 60th anniversary of President Truman's creation of the National Security Agency. As a key member of the Department of Defense, the National Security Agency has provided critical intelligence and support to our warfighters throughout its history. The dedication and skills of your truly joint workforce, a cross-section of the Nation's population represented by Department of Defense Civilians and uniformed members of every Military Service, have directly enabled our country's military successes and have saved innumerable lives.

On behalf of the members of the Armed Forces, I congratulate the National Security Agency on 60 years of outstanding service to the Nation.

Sincerely,

Congratulations Keith on your leadership and the great work of NSA.

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

JUN 15 2012

General Keith B. Alexander, USA
Director, National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6242

General Alexander:

Please accept my congratulations on the 60th anniversary of the creation of the National Security Agency. Over the years, and especially during the conflicts in the Middle East, NSA has played a significant role in protecting our Nation and its troops from harm. NSA has done an exemplary job of securing our troops' communications and providing vital, life-saving information on foreign adversaries, consistently giving our engaged forces at all echelons the upper hand in combat situations.

As you celebrate the 60th anniversary of the National Security Agency, I congratulate you and the Soldiers, Sailors, Airmen, Marines, Coast Guard Sailors, Civil Servants and Defense Contractors of NSA on a job well done and on behalf of the Defense Intelligence establishment offer my best wishes for continued success in this vital mission.

Michael G. Vickers

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

JUN 04 2012

General Keith B. Alexander, USA
Director, National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6242

Dear General Alexander:

I am pleased to extend my congratulations on the 60th anniversary of the creation of the National Security Agency. As a member of the Intelligence Community, NSA has played a key role in intercepting our adversaries' communications and securing and protecting our own. As the threat environment changes significantly in the 21st century, I look forward to NSA's continued efforts to collaborate across the Intelligence Community to ensure our success in protecting our nation and its citizens.

Please accept my congratulations on a job well done as you celebrate the 60th anniversary of the National Security Agency.

Sincerely,

Jim Clapper
James R. Clapper

I "grew up" in the SIGINT business — including two tours at NSA, as well service on the Advisory Board. I have a special place in my heart for the Agency, and its superb people.

Foreword
3

An Agency is Born
10

Decade of Change
28

Advances in Technology
50

A Period of Growth
68

The End of an Era
80

Adapt and Adjust
94

An Agency Rich in Heritage
112

NSA Timeline • 1952 to 2012
114

NSA and CSS Seals Description
116

AN AGENCY IS BORN

National Security Agency

1950s

Today, if you head north on Interstate 95 and exit on Rt. 32 towards Annapolis, you will find yourself on a dual lane highway that passes old Rt. 1 and then begins to rise up a small hill. As you reach the crest, you cannot help but notice a collection of buildings off in the distance.

In daylight, the area – save for the wide array of towers and satellite dishes – could well be mistaken for a corporate campus of a Fortune 500 company. Those who live in Central Maryland are well aware of this organization's existence, but those viewing the area for the first time might not easily guess that they are passing the headquarters of the National Security Agency, an organization that for more than 60 years has provided and protected our Nation's most important communications.

At night, the same area takes on an eerie glow. To many, the image of the buildings speaks of power and vigilance; to others, the vision imparts a sense of mystery and secrecy. Despite the many perspectives on its purpose and mission, one thing is certain - NSA has played a critical and indispensable role in securing our Nation.

Today, NSA's thousands of affiliates around the world, both military and civilian, employ the latest methods and technologies to accomplish its mission. In the beginning, however, there were no buildings or people or technology. In the beginning there was only Lieutenant General Canine.

March 17, 1953. Flag presentation: (L to R) Major General George A. Horkan, Quartermaster General, USA, presents a three-star flag to Lieutenant General Ralph Canine in honor of his promotion and appointment as Director of the National Security Agency.

Lieutenant General Canine

Born in Flora, Indiana, in the late 19th century, Ralph J. Canine had entertained thoughts of becoming a doctor, but America's entry into WWI prompted him to change his career plans. Canine entered the Army as a second lieutenant and stayed on after the Armistice was signed. During WWII, he was appointed Chief of Staff for XII Corps under the command of General George S. Patton, and after the war, he served for a time as Commander of the famed 1st Infantry Division.

Despite having scant experience in the realm of intelligence, 1951 found him as head of the fledgling Armed Forces Security Agency (AFSA), an organization created after the war to streamline and consolidate the Nation's cryptologic assets. However, AFSA was unable to achieve its desired purpose, and a new approach was needed.

Due to the efforts of the Truman administration, AFSA transitioned into the newly created National Security Agency (See Document A-1 and A-2 at end of chapter). In 1952 when the Agency was formally signed into existence, Canine was named its first Director. Smart, experienced, and practiced in sound management principles, Canine began to mold the new entity into an effective organization. Time would demonstrate that he was the right person for the job.

LTG Ralph J. Canine
The first National Security Agency Director

Infused with a sense of both urgency and dedication to his mission, Canine quickly began to use the new authorities given him by President Truman and the Secretary of Defense to create a stronger cooperative effort between NSA and the Service Cryptologic Components (then called "Agencies"). He also successfully advocated for budget supplements to pursue research and to purchase computers and communications infrastructure components.

Aware of the other agencies' challenges to his young organization's mandates, he frequently tangled with other leaders in the Intelligence Community, starting with his parent organization at the Department of Defense (DoD). He was particularly at odds with the CIA over several issues, especially CIA's failure to inform him about operations that infringed on NSA's activities, which included a CIA attempt to create its own Signals Intelligence (SIGINT) system.

While Canine was adept at fighting off the outside forces that threatened the new organization, he was even more skilled at developing the critical internal elements of NSA, particularly morale. He interacted regularly and directly with employees and successfully infused both the civilian and military members of the workforce with a strong esprit de corps.

One of Canine's senior subordinates said he "raised the National Security Agency from a second-rate to a first-rate organization." Most importantly, Canine's hard work and vision established the foundation of an Agency that, unlike AFSA, would provide America's leaders with the cryptologic support they needed to meet the challenges of the Cold War and beyond.

After the surrender of Japan in 1945, the victorious Allied powers enjoyed a brief respite

from hostilities. By 1947, however, the hostility between the Soviet Union and the United States had grown to such a degree that it was referred to as "the Cold War." In 1950, the conflict would turn hot on the Korean Peninsula, and one of NSA's first challenges would be to support the efforts of the United States and its Allies in "The Land of the Morning Calm."

Korea

The Korean War began in the early hours of June 25, 1950, when the forces of communist North Korea invaded South Korea. Within days, the United States had committed itself to restoring the Republic of Korea in the south and had persuaded the United Nations to join the endeavor.

By month's end, the North Korean offensive had forced the U.S. 8th Army into a defensive position. Although 8th Army commander General Walton H. Walker's situation was extremely tenuous, he was committed to holding the line. With the twin resources of effective SIGINT to assist him in making the right moves in keeping the perimeter secure and sound communications security (COMSEC) to protect his own communications from being exploited, Walker was able to maintain his position.

American strategic-level communications during the operation remained safe from the enemy due largely to the dependable communication tools such as the SIGABA device and the M-204.

During the early difficult days of the battle, Walker had firmly remarked to his 25th Division staff, "I want everyone to understand that we are going to hold this time. We are going to win." Thanks to the dogged determination of the UN forces, and effective SIGINT and COMSEC, Walker would remain true to his words.

While there had been no intercept or analytic coverage of North Korea before the war, the same was not true of China. The U.S. had been providing communications intelligence (COMINT) on the Communist Chinese since General Marshall's attempt to broker peace in the Chinese Civil War in 1946. In fact, China was

LEADERSHIP

DIRECTORS

LTG Ralph J. Canine, USA (July 1951 – November 1952)

Lt Gen John A. Samford, USAF (November 1956 – November 1960)

VICE DIRECTORS

RADM Joseph Wenger, USN (December 1952- November 1953)

Brig Gen John Ackerman, USAF (November 1953 – June 1956)

Maj Gen John A. Samford, USAF (June – August 1956)

DEPUTY DIRECTORS

Joseph H. Ream (August 1956 – October 1957)

Dr. Howard Engstrom (October 1957 – August 1958)

Dr. Louis W. Tordella (August 1958 – April 1974)

AFSA was responsible for supplying the Army's codes and ciphers, Korea, 1950s

one of the major production areas in the early 1950s, with coverage of both the Communists and the Nationalists.

As the Korean War went on, analysts at AFSA developed information from Chinese messages about the movement of crack Chinese units from central China to the coast and then to Manchuria. COMINT provided information on the units and number of Chinese troops poised on the China-Korea border, although there were no intercepted messages saying the forces were to cross into Korea.

The Korean War was a watershed time for the United States. Before the outbreak, U.S. policy had been to downsize the military and intelligence services. Policy changed virtually overnight to one of rapid and expansive buildup.

This changed policy affected NSA as well. The National Security Council in July 1950 approved a sizeable increase in hiring for AFSA, which continued into the NSA era, well after the end of the war.

Lieutenant General Samford

In the fall of 1956, LTG Canine retired, and Lieutenant General John A. Samford, USAF, was appointed NSA's second Director. Like Canine, Samford could claim an impressive military career. Unlike Canine, by the time he was promoted from the position of NSA Vice-Director to the head of NSA, he had several years of Intelligence Community experience under his belt. A 1928 graduate of West Point, Samford served as Chief of Staff of the 8th Air Force during WWII, and in the postwar period as Chief of U.S. Air Force Intelligence.

Like his predecessor, Samford possessed a wide range of experience and management skills; however, while Canine was known for using the stick, Samford was much more inclined to use the carrot. Samford's preference for diplomacy rather than confrontation eventually led to improved relations between NSA and its partners in the Intelligence and Defense Communities. Ironically, Samford had initially been opposed to the creation of NSA, yet proved to be one of its most effective leaders.

Move to Civilian Deputy Director

In addition to building on Canine's success, Samford established the tradition of a civilian rather than military Deputy Director. The AFSA practice of having military vice-directors continued when General Canine was the Director of NSA despite President Truman's 1952 memorandum calling for a civilian NSA Deputy. When Canine retired, however, General Samford appointed a civilian Deputy. At the time, the Eisenhower administration's preference was to bring nongovernment expertise into federal departments, and Agency leadership was prompted to select a civilian deputy from outside NSA. Joseph Ream came to NSA from CBS Broadcasting. However, as a noncryptologist, he faced a stiff learning curve. When this challenge was compounded by family illness, he resigned.

Dr. Howard Engstrom, a naval officer who worked cryptology during WWII, was Ream's successor. After the war and a period as vice president at a private corporation, Engstrom served as Associate Director and Director of NSA's Research and Development Organization.

A year later, he was appointed NSA's Deputy Director, a position he held for less than a year before returning to private industry.

Agency leaders began to understand the need for cryptologic experience at the top. General Samford successfully argued that if he was to have a civilian deputy, it needed to be an "insider." With this goal in mind, Samford selected Dr. Louis Tordella. It would prove to be an excellent choice (Tordella would go on to become NSA's longest serving Deputy Director). Tordella had a Ph.D. in mathematics and had worked in both cryptanalysis and communications security. Further, he had been manager of a high-profile technical project, and served in the Pentagon office that controlled NSA's budget. Most importantly, he was ready to serve as the Director's sounding board, an important consideration for Samford. The original concept had been for a civilian to hold office for only a few years, and then move on. As it happened, Dr. Tordella served almost 16 years, establishing a long list of accomplishments and an enduring legacy of leadership.

Tested by Crises

During Samford's directorship, NSA provided critical cryptologic support in several crisis situations in the Middle East and Eastern Europe, such as the Suez Crisis and the 1956 revolt in Hungary.

The Suez Crisis rose out of U.S. and international concerns over Egypt's aggressive move to nationalize the Suez Canal, at that time owned by a French and British company. The canal was of great importance to the economic development of both nations, and they considered it vital to their national security, due to its strategic geographic location. At the same time, Egypt was increasingly turning to the USSR as an ally.

NSA intelligence reporting at the time showed Soviet shipments of military materiel to Egypt and Syria. While the U.S. was pursuing anti-communist and anti-imperialist policies, Britain – though anti-communist – was equally determined to retain its status and influence as an imperial power, particularly in the oil-rich Middle East.

An Israeli assault on the Sinai and an ensuing British and French bombing campaign temporarily restored British control of the Canal Zone, but the U.S. – working through the UN – forced a ceasefire and an eventual withdrawal of French and British forces. Egypt retained control of the canal, although it agreed not to restrict shipping.

Hungary, like other East European countries, suffered under the yoke of post-World War II Soviet occupation and domination. In 1956, discord erupted into rebellion in Budapest. The Soviet response using tanks and troops was a ruthless squelching of the revolt. As the situation heated up and hostilities erupted, NSA was quick to supply President Eisenhower and his senior staff with an accurate picture of Soviet movements.

After the uprising subsided, there was some criticism that COMINT should have provided more warning before the crisis. In fact, there were some COMINT indicators, but at that time NSA was not authorized to analyze intercepts; NSA's role was simply to forward the information to other intelligence agencies.

The Move to Ft. Meade – 1957

The latter part of the 1950s witnessed NSA's growth in both size and importance. When NSA was created, the assumption was that in time the new entity would establish new headquarters to unify its many important but disparate parts. In short, NSA needed a home – but where? At its inception, NSA was split between different locations and facilities. AFSA/NSA's headquarters were in the Naval Security Station on Nebraska Avenue in the District of Columbia, as were the cryptographic functions. However, the COMINT functions were located at Arlington Hall Station, the Army's cryptologic headquarters in northern Virginia.

These military posts were already crowded, and the geographic division of the two principal functions created management

The Move to Fort Meade

"Meade Mobile" provided information on relocating to the Fort Meade area for employees.

A great deal of preparation went into the move to Fort Meade. Employees were offered field trips to look over the construction of the new buildings and given all the information they could use to line up housing and address the challenges associated with the transition.

Once in place, the workforce appreciated the newly constructed facilities after existing in structures hastily thrown up early in World War II. The new buildings had several interesting features, including what was reputed to be the country's longest unobstructed corridor. Offices were linked by a 99 station pneumatic tube system. And, particularly attractive to the young workforce, there were snack bars, with hot grills, on alternate floors. ■

challenges. In addition, after it was known that the USSR had exploded an atomic bomb, the government began dispersing key agencies to ensure their survival in case of a surprise Soviet atomic attack on the capital. AFSA/NSA was one of those key agencies.

A planning committee recommended that Fort Knox, Kentucky, be a permanent home. It was away from likely atomic targets and well protected. Planning for a move to Kentucky began, but there remained two serious obstacles. First, many in NSA's leadership felt that a location so remote from Washington would prevent effective interaction with DoD and other intelligence agencies. Second, there was considerable resistance within the cryptologic workforce to a move that would involve such dislocation of families.

These challenges ultimately proved too great to overcome. The planners rethought their options and decided that Fort George G. Meade in Maryland offered a workable solution. It was considered far enough away from the expected blast zone around Washington to meet the survivability requirement. The move to Maryland was approved, and NSA began occupying buildings on Fort Meade in the late 1950s. Fort Meade has remained NSA's headquarters ever since.

Leadership anticipated that the initial building would unite both halves of NSA's mission at Fort Meade. However, NSA quickly outgrew the building. NSA, along with other intelligence and defense components, expanded rapidly during and after the Korean War. The initial building even proved too small to contain the entire COMINT workforce. Planning and construction of additional buildings began soon after the first was finished. The COMSEC organization remained in D.C. until a new building was completed on Fort Meade in 1968.

Recruiting a Qualified Workforce

Finding a new home was only one of the many challenges NSA faced during its formative years. Because cryptology is a unique profession, NSA faced considerable

National Security Agency, circa 1950.

difficulty in recruiting and retaining qualified employees for its specialized workforce. Typically, personnel from the Service Cryptologic Agencies did not stay long after converting to civilian status. To add to the recruitment challenge, none of NSA's job descriptions were in the Civil Service Registry. Throughout the 1950s, NSA pushed to have recognition as an "excepted service," with hiring and firing authority and the ability to define its own jobs. President Eisenhower supported this approach. Eventually, NSA's hiring and firing authority was granted through the enactment of Public Law 86-36, "National Security Act of 1959."

A World-Wide Cryptologic System

In the late 1940s and early 1950s, as the dimensions of the Cold War became apparent, NSA and the uniformed services moved from a collection focus on Germany and Japan to sites better situated for collecting signals from the USSR, Eastern Europe, China, and North Korea.

Over time, NSA asserted control over location surveys, a prerequisite to establishing physical locations for new sites. Consequently, NSA was able to influence where the Service Cryptologic Agencies established their field sites.

Eventually, a three-tier COMINT system emerged worldwide, driven by needs for COMINT and the communications capacities of the era. Forward sites collected and processed any "take" that was time-sensitive and could be handled without sophisticated equipment. Intermediate stations, often at theater level, dealt with material that needed more processing but still had to be distributed quickly. Intercept that required processing on massive computer banks or needed only for long-term study was sent to NSA. In addition, the Navy and Air Force operated mobile collection platforms that fed intercept into the system at appropriate levels.

To serve worldwide customers, particularly the major military commands in Europe

and Asia, NSA established the role of senior representatives in Europe and the Pacific.

On the protect side, when President Truman established NSA in 1952, he created a central board for COMSEC policy. However, this board never materialized and eventually NSA assumed responsibility for COMSEC. In October 1953, a year after NSA was established, the National Security Council gave NSA authority in COMSEC technical matters, although policy direction and budgeting still came from a special board.

One major COMSEC project begun at AFSA continued at NSA. At the end of World War II, the government needed a replacement for the SIGABA/ECM, the highly sophisticated cipher machine used by both the Army and Navy. After 1949, AFSA began developing a device that would be smaller, lighter, faster, and economical. The device, the KL-7, was ready by the early 1950s.

NSA looked in-house to develop its next cutting edge device, the KW-26, to secure teletype or other kinds of record communications. It employed the latest technology and electronic online encryption and could withstand combat conditions. The U.S. military now had strongly protected communications. Over 14,000 units were used into the 1980s.

NSA did not stop there. It now looked to more advanced machine systems for enciphering text messages and safeguarding speech privacy.

Dwight D. Eisenhower

In 1953, the man who led America and the Allies to victory in Europe in World War II, Dwight D. Eisenhower, ascended to the presidency. The United States had faced grave perils during WWII, but now America and the world faced not only the prospect of conflict with the Soviet Union, but also the threat of nuclear war.

From its earliest days, the Eisenhower administration was deeply concerned about the possibility of a surprise attack on the United States by the Soviet Union and reducing the drain of DoD appropriations on the annual budget. The President convened a number of panels and committees to study how these seemingly incompatible goals might be achieved.

The President also commissioned a study of defense matters by Dr. James Killian, president of the Massachusetts Institute of Technology. Among other things, Killian recommended that NSA be strengthened, because awareness of an imminent attack would most likely to come through COMINT sources.

The Eisenhower administration had two personnel concerns that involved NSA and

Second Party Partners

In 1940, before the United States entered the war, the U.S. and Britain began exchanging sensitive information about their cryptanalytic efforts against Germany and Japan. Sharing became especially close in the war years, and eventually this relationship was extended to include Canada, Australia, and New Zealand.

Shortly after the end of the War, President Truman authorized the COMINT agencies to continue this relationship with the UK. The initial 1946 BRUSA (British-United States) Agreement was revised in 1952 (as the UKUSA [United Kingdom-United States] Agreement), reflecting the realities of the new Cold War. Both countries knew they had advantages the other lacked and that their need for each other was nearly as great as it was during the War. A strong motivation for this partnership was the threat posed by growing Soviet political and military aspirations. This threat was compounded by Soviet efforts in Europe and elsewhere to expand Communist interests, control, and influence. These ambitions drove the U.S. national policymakers' intelligence needs. NSA had to evolve from maintaining a wartime operations

the Service Cryptologic Agencies. First, the administration was worried about the potential security risks of the number of people who had access to COMINT. A commission on government organization chaired by former President Herbert Hoover found that almost 30,000 Americans were cleared for COMINT. Of this number, not more than 5,000 were consumers of the product – the majority were producers. The administration recommended reducing the number of people with COMINT access and strengthening security procedures.

In 1957, the Eisenhower administration asked Deputy Secretary of Defense Reuben Robertson to chair a high-level committee to review spending on COMINT. Although initially committed to radical funding reductions, Robertson came to appreciate the value COMINT had in decision making. At the end of the study, the Robertson Committee proposed two principal recommendations.

The Committee's first recommendation was to consolidate some collection stations to eliminate duplication. The second had farther-reaching consequences. Robertson recommended that all budget lines for cryptologic activities be centralized under the Director of NSA. This move was implemented in 1959 by the creation of the Consolidated Cryptologic Program (CCP). With only a few changes, it has continued as the principal budgeting process for the cryptologic community.

The KL-7, originally the AFSAM-7

tempo to developing and sustaining a new level and type of effort reflecting the evolving needs of Cold War era policymakers.

The actual rate of success achieved by this partnership is still classified, but it is known that valuable intelligence was extracted from unencrypted Soviet communications. As a result, senior leaders in the U.S. and the UK jointly received more robust intelligence.

The combined efforts of America and its post-war allies led to numerous successes. One of the most impressive was the VENONA project, which not only clearly demonstrated the prowess of Soviet cryptologic systems but also showed an uncanny ability by the combined Western intelligence agencies to overcome seemingly insurmountable challenges. By overcoming and solving such immense problems, NSA began to build a solid reputation. ■

VENONA

The VENONA project was one of the great cryptologic triumphs of the Cold War. The effort was a "compartmented" (i.e., restricted access) operation targeting Soviet diplomatic traffic. The Army initially began analysis of this material during World War II, and quickly realized it had been enciphered on a one-time pad system. (Webster's defines a one-time pad as a "system of random additive or mixed key in sequence that is used one time and then destroyed.") Used properly, the system is virtually unbreakable.

The newly-established NSA took on the challenge of gleaning intelligence from the "unbreakable" VENONA traffic previously analyzed by the Army. Through what was described in 1995 by NSA Deputy Director William P. Crowell as a "brilliantly intellectual cryptanalysis effort," skilled British and American cryptanalysts uncovered some anomalies indicating a solution might be possible. They found that, under wartime pressures, Soviet communicators had re-used some one-time pads. This discovery was critical because pads that had been used twice were vulnerable to decryption. Further detailed analysis also disclosed that the communicators belonged to Soviet espionage services: the GRU, Soviet military intelligence and the KGB's predecessor organization. Although the Soviets changed their encryption system, they could not retrieve the accumulated diplomatic traffic being exploited at NSA. This accumulated traffic revealed many intelligence secrets over the following years.

Julius and Ethel Rosenberg at their trial in March 1951. As a result of information gleaned from the Venona project, they were found guilty of treason and executed.

Throughout the life of the VENONA project, U.S. and British crypto-linguists recovered portions of thousands of messages. Gradually, a picture of a massive Soviet espionage effort that posed a very real and significant threat to national security began to emerge. This discovery was alarming. The Army and NSA shared decrypts with the FBI. The firm condition that NSA imposed on the FBI was that the material that had been decrypted could not be used in court, or otherwise be made public. Although NSA was committed to keeping the Nation safe, protection of sources and methods, as well as civil liberties, mandated that these foreign intelligence successes could not be revealed.

NSA kept working on VENONA messages until 1980. At that time, it was decided the cost of continuing the program outweighed any possible benefits, and the project was closed down. The FBI kept its side of the bargain, and VENONA stayed under wraps until 1995, when it was officially declassified by the U.S. Government. ■

Other distinguished members of the scientific and technological community, including Dr. William O. Baker from Bell Laboratories, reviewed NSA operations. Baker and his panel recommended that NSA be split into a think tank and an operational component. Eisenhower did not agree, but liked Baker's concept of a cryptologic think tank. Consequently, the President personally supported the establishment of a high-level cryptologic research component under the auspices of the Institute for Defense Analyses in Princeton, New Jersey.

Over the years, Baker's idea paid high dividends in terms of theoretical research into cryptology and computers, much of which was subsequently turned into practical applications for crisis support. The importance and indispensable contribution of cryptologic think tanks continues to this day.

NSA's business did not end with COMINT. Electronic intelligence (ELINT) was exploding as our adversaries employed more and more weaponry and systems emitting non-communications signals. NSA needed to exploit this intelligence but needed an effective system. The system as it existed was fragmented because each military service had its own processes.

Understanding the pressing need for consolidation of the two systems, Eisenhower gave NSA the authority for both strategic analysis and reporting of ELINT. As with COMINT, each service kept a tactical capability, but the system was no longer fragmented. The melding of COMINT and ELINT led U.S. intelligence personnel to speak of SIGINT and to treat it as an independent discipline.

As the crises of the Cold War continued, President Eisenhower was concerned that he was not receiving information about crisis events fast enough. He set a standard for critical information to reach the President's desk – ten minutes after recognition. This standard was to be achieved through use of a Critical Communications system, called CRITICOMM; priority messages on this system later came to be called CRITICs.

A study determined that the U.S. SIGINT System had the best communications in the government. It had been operating 24/7 since World War II, and, moreover, many sites where CRITICs would be produced already belonged to the system. Dr. Louis Tordella, soon to become the Deputy Director of NSA, was assigned to develop a plan and brief CRITICs to the President. He described the plan and its costs at a meeting of the National Security Council. After Tordella finished talking, Eisenhower asked a DoD senior executive with communications expertise if the plan could be achieved, and when told it was feasible, merely said, "Let's do it." To get it done, the SIGINT System needed extensive upgrading. Through NSA's determination and effort, Eisenhower's goal of a ten-minute standard was met in 1963.

The Great Leap Forward

As the 1950s came to a close, the National Security Agency had become one of the most important components of the United States' defense against the Soviet threat. However, the challenge posed by the Soviets, while daunting, was only one of many. During WWII, American industry had produced the machines and devices necessary to win the war. Superior technology had given the Allies a great advantage, but the need to keep pace and surpass the Soviets gave impetus to even greater achievements in the technological realm.

Many argue that the first operational computer was the COLOSSUS, designed by the British to exploit a high-grade German machine encryption system. Whether or not it is correct that COLOSSUS was the first computer, the Allies accrued considerable experience with machine processing during World War II.

By the mid-1950s, however, things had begun to move at even greater speed. The computer age had fully arrived, and new concepts and systems that allowed both military and civilian organizations to do things faster and more efficiently were quickly becoming the rule. As the cryptologic community began to learn of developments in computing at a number of universities, technical experts at NSA and

LTG Ralph J. Canine, USA (left) congratulates Dr. Louis W. Tordella, NSA's first civilian and longest-serving Deputy Director.

in the military began to devise ways to apply computers to cryptologic work and to design machine support systems directly applicable to specific targets.

NSA needed computers for cryptanalytic processing of foreign systems, compiling cryptomaterials for U.S. use, and for distributing intercept and reports. As a result, NSA adopted the goal of developing a general-purpose computer.

This effort gave rise to the NSA Scientific Advisory Board (NSASAB), a group of security-cleared scientists and academics from outside the government who met annually to help NSA understand the latest developments in technology and incorporate them into cryptologic work. At a 1954 NSASAB meeting, the members were asked, "What are things you dream about, but do not dare hope for?" The answer came back clearly "more speed in smaller boxes." The only point of disagreement among board members and NSA technologists was the magnitude of computing power to be set as their goal. This goal led directly to an accelerated program of computer development.

President Eisenhower himself believed that NSA's development of robust computer power and speed would be essential to its continued ability to meet national requirements, particularly in warning. He authorized the use of his name in recruiting specialists in the field.

In 1956, the DoD approved an extra $5 million above normal budget limits for the next five years to develop high-speed computers. The goal was achieved in the early 1960s with a system named HARVEST.

The 1950s were important years for NSA in computers. In 1955, NSA purchased one IBM computer, which later came to be called the HARVEST system and proved pivotal to NSA's future successes. NSA made this purchase after a one-year study that revealed that the cost of running the computer was $51.78 an hour, while a person cost $15.02 an hour (see Document B at end of chapter). Nevertheless, the study ended with a recommendation to purchase a HARVEST because it predicted that NSA could manipulate and program the computer to eventually be faster and more economical than a person. This prediction turned out to be correct. The technology quickly transferred outside NSA and became an important factor in commercial computer development and academic research. Such transfers of technology happened frequently over the ensuing decades and continue to this day.

Pleased with its initial forays into the computer age and anxious to maintain its leadership in the field, NSA was quick to adopt technology and advancements from outside sources. For example, NSA substituted transistors for vacuum tubes, an efficient and economical move. Also, in-house or contracted research resulted in several innovations, such as remote-access systems and advanced data storage methods. The initiatives NSA took in this decade established its determination to push the technological envelope and stay at the cutting edge of technology. ■

National Security Agency
Historic Documents

Document A – Framework for NSA, 1952, pages 1 and 4

Document B – Excerpts from a study on the purchase of the HARVEST System, 1957

DOCID: 3978768

TOP SECRET

SECURITY CLASSIFICATION (If any)

TOP SECRET - SECURITY INFORMATION

DISPOSITION FORM

Declassified and approved for release by NSA on 06-14-2012 pursuant to E.O. 13526

FILE NO.	SUBJECT
	Initial Plans Effecting National Security Agency (NSA)

TO	FROM	DATE	COMMENT NO. 1
Chiefs, Staff Divisions and Offices	Chief, Plans and Policy Division	31 Oct 1952 Col. Gregory/60532/iew	

1. National Security Council Intelligence Directive Number 9 (revised) 24 October 1952 authorizes the replacement of the present Armed Forces Security Agency by a National Security Agency. This change will have little effect on the general broad missions and functions of AFSA and should not necessitate any major readjustments in personnel. Major readjustments of a policy and procedure nature which will affect the several Services, other consumers, and to some extent, other governmental agencies are anticipated. These will be felt in such fields as Logistics, Training, Research and Development, Command Relations, etc.

2. It is necessary that the Director, AFSA, be provided certain initial concepts, philosophies, and plans for effecting the change from AFSA to NSA. The Chief, Plans and Policy Division has been directed to establish certain committees and to coordinate the assembly and final production of a position paper for the Director.

3. As initial guidance, the Director has announced the following listed basic criteria which he considers desirable. Additional broad guidance will be found in "Joint Action Armed Forces" (FM 110-5, JAAF, AFM 1-1).

a. No joint units should directly support uni-service field activity; i.e., Army units will normally provide COMINT for a field Army.

b. Operations to be decentralized.

c. Control to be centralized and established along well defined command lines.

d. Establishment within NSA of strong area sub-organizations with clear and concise channels of communications and with limited operational control authority over Service COMINT organizations within the area; i.e., NSA, Europe; NSA, Far East, etc.

e. Delegation of operational control of COMINT units to Service field commanders when such units are engaged in close support operations (see JAAF).

f. Operational control of COMINT units, other than those specified in e. above, may be delegated to NSA area organization commanders.

4. The following assignment of tasks and committees as announced during the orientation and planning conference on 31 October is confirmed:

a. Determination of Basic Organizational and Operating Concepts for Control of Supporting Activities - Determine the optimum practicable concepts, doctrines, and procedures for the organization and operation of NSA. This includes the exercise of operational and technical control over activities of the Government

DD FORM 1 FEB 50 96 REPLACES NME FORM 96, 1 OCT 48, WHICH MAY BE USED.

16—54801-8 ★ U. S. GOVERNMENT PRINTING OFFICE

TOP SECRET

Document A-1: Framework for the new National Security Agency, October 1952, page 1.

DOCID: 3978768

~~TOP SECRET~~

~~TOP SECRET - SECURITY INFORMATION~~

Initial Plans Effecting National Security Agency (NSA)

Chiefs, Staff Divisions and Offices | Chief, Plans and Policy Division | 31 Oct 1952 | COMMENT NO.1

1. Administrative Control - Determine the extent to which it will be necessary and/or desirable for the Director, NSA, to exercise administrative control over COMINT activities including facilities and personnel of the Department of Defense.

COMMITTEE: Captain E.S.L. Goodwin, USN, Colonel George E. Campbell, USA

m. Relationships with Department of Defense Agencies - Recommend desirable arrangements for maintaining necessary relationships with agencies of the Department of Defense such as the Research and Development Board, and the Munitions Board.

COMMITTEE: Dr. S. Kullback - Research and Development Board
Colonel Shaw - Munitions Board

n. Revision of USCIB Directives No. 1, 2, and 3 - Prepare appropriate papers recommending the revision of USCIB Directives 1, 2, and 3. Set forth criteria and desirable qualifications for the Executive Secretary, USCIB. Recommend the size and general functions and responsibilities of the USCIB Staff. Recommend in broad terms the procedures which should be used by USCIB. (See paragraph 1g, NSCID No. 9)

COMMITTEE: Hamill D. Jones

5. National Security Council Intelligence Directive Number 9 is available for examination on a need-to-know basis in the office of the Chief, Plans and Policy Division. Other assistance including stenographic and reproduction facilities will be available in Room 19-236, NAVSECSTA. Matters concerning this project should be referred to Colonel J. O. Gregory or LCDR C.T.R. Adams, Plans and Policy Division, Code 131, Extension 60532.

FOR THE CHIEF, PLANS AND POLICY DIVISION:

RUSSELL H. HORTON
Lt. Colonel, Signal Corps
Assistant Chief

Copy to each individual named herein.

4

~~TOP SECRET~~

Document A-2: Framework for the new National Security Agency, October 1952, page 4.

~~CONFIDENTIAL~~

Declassified by D. Janosek, NSA/CSS
Deputy Associate Director for Policy and Records
on 15-10-2010 and by [illegible]

TABLE II

UNIT COSTS, BASED ON RENTAL ESTIMATES x 50

NSA: R/D vs M/O, and AEC

ITEM	NUMBER TOT.	NSA R/D	NSA M/O	AEC	COST ÷ 1000 NSA R/D	NSA M/O	AEC
Computer	1	1	0	1	5,000*		4,000*
Memory - M.S	8	1	7	4	1,100	7,000	4,000
Memory - H.S.	4	1	3	2	1,700	3,000	2,000
Register - H.S.	16	1	15	16	70	1,050	1,120
Exchange	1	0	1	1		1,500	1,500
Card Punch	1	0	1	1		50	50
Card Reader	1	0	1	1		50	50
Printer	1	0	1	1		100	100
Mag. Tape - H.P.	6	1	5	0	430	500	
Mag. Tape 727	4	0	4	4		120	120
Mag. Disc. - H.P.	1	0	1	1		250	250
			TOTAL		8,300	13,620	
			NSA TOTAL			21,920	
			AEC TOTAL				13,190

* The difference in estimated cost of NSA vs AEC Computer portion is based upon the following:

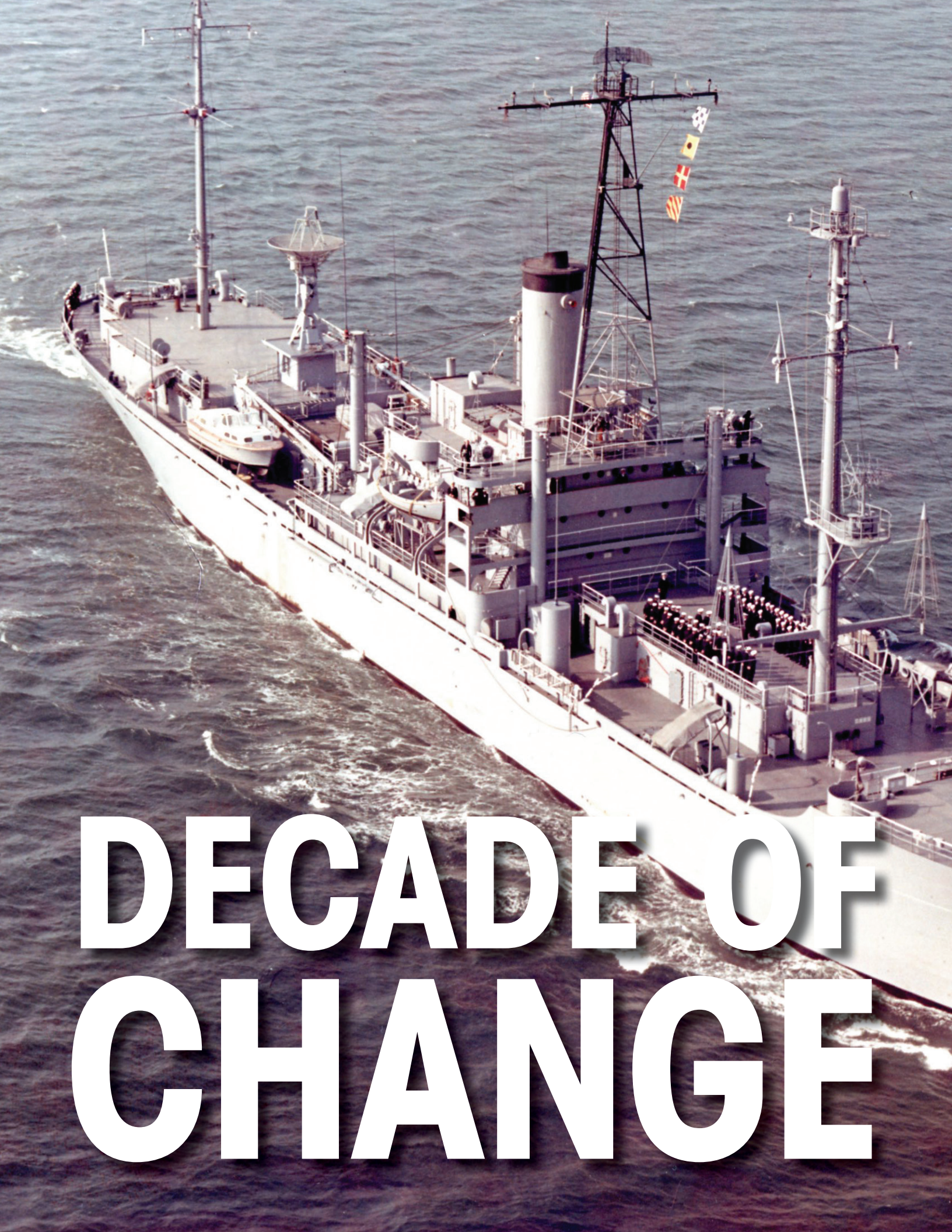
DEVELOPMENT: About a year, and $600,000 have been devoted to generating the special features required by the NSA problem study. AEC logical development effort will be almost negligible.

CONSTRUCTION COST: HARVEST design provides for three Stream Units, complex automatic addressing and table extraction, and elaborate indexing. AEC's computer will not require these features, but will have a high-speed arithmetic unit not expected to be in HARVEST. Estimated additional construction cost of HARVEST: $400,000.

~~CONFIDENTIAL~~

Document B: Table from a six-page study conducted on the purchase of the HARVEST System in 1957. This study revealed the cost for the computer was $51.00 per hour and a person was $15.00. (This analysis is on the DVD.)

Arlington Hall Station, the Army's cryptologic headquarters in northern Virginia, circa 1950.



DECADE OF CHANGE

1960s

By the 1960s, NSA was regarded as a vital element in the effort to provide U.S. policymakers and war fighters the critical intelligence needed to successfully complete their missions. While NSA entered the '60s with pride in its accomplishments, the decade would not be without its challenges. NSA sought out the best and the brightest to meet these challenges. (See Documents A1 & A2 at end of chapter.) Early in the new decade, the Agency would also realize the importance of loyalty in the workforce.

Martin and Mitchell

Then and now, intelligence agencies operate on the premise that the information they collect will be kept secret. To accomplish this requirement, vast sums of money are spent on tangible devices to secure and protect the environment in which the information resides. However, physical security measures can only do so much. In the end, every intelligence organization depends on the integrity of its workforce to protect its sensitive information.

In June 1960, Bernon F. Mitchell and William Martin, two NSA employees, applied for annual leave to visit their families on the West Coast. That was what they told their superiors. Instead, the pair traveled to Mexico City, then to Cuba, and eventually to the USSR.

Soon after, they surfaced in Moscow as the main attraction of an international press conference sponsored by the Soviet Government. Their actions came as a shock to NSA and the United States. As the event unfolded, it became clear that the point of the proceedings was to provide a forum for the men to describe in detail NSA

USS Liberty

operations, including activities that involved the monitoring of the communications of some of America's allies.

Alarmed by the actions of the pair in divulging NSA's critical information, President Eisenhower ordered an investigation of the incident that culminated in a comprehensive report. The 13-month study revealed that Martin and Mitchell were mathematicians, first with the Naval Security Group and, from 1957 to 1960, as NSA civilian employees. Both men had become disaffected with U.S. policy toward the Soviet Union as the Cold War developed and together made the decision to defect.

Ultimately, life in the Soviet Union proved to be disappointing, but their attempts to return to the United States were thwarted by their inability to obtain immunity from prosecution. Martin died in Tijuana, Mexico, in 1987; Mitchell in St. Petersburg, Russia, in 2001.

The Martin and Mitchell defection of 1960 had strong repercussions. Due to the incident, NSA tightened its hiring and security practices to include full background checks and polygraphs.

Bearing the Burden

The decade of the 1960s for the National Security Agency and America began with hope and confidence in the future. This optimism was tempered, however, by the Soviet threat and the even more ominous menace of nuclear war. In his 1960 inaugural speech, President John F. Kennedy spoke to this dichotomy noting that "mankind holds in his mortal hands the power to abolish poverty, but also the power to abolish human life." Kennedy was equally adamant, however, that despite the challenges the United States faced, America would "…bear any burden and endure any hardship… to ensure the survival and success of liberty."

NSA proved to be a crucial part of this effort under the strong leadership of Army, Navy, and Air Force Directors. All of them had experienced the crucible of war, and all were imbued with a sense of commitment and dedication to their country. In the beginning, NSA was the sum of many

(Left) William Martin and Bernon Mitchell (center) tell Moscow press why they defected. (See attached DVD for audio and transcript)

parts; however, over time it began to develop its own unique identity. In early 1963 NSA adopted a seal that proclaimed the Agency a component of the Department of Defense. Two years later, Lieutenant General Marshall S. Carter, USA, the new Director of NSA, wanted to emphasize that the Agency served the needs of the entire U.S. Government, even though it was subordinate to DoD. Consequently, he had a second seal prepared that incorporated this idea into the new design.

Vice Admiral Frost

In the fall of 1960, NSA would see its first U.S. Navy Director, Vice Admiral Laurence Frost. A native of Fayetteville, Arkansas, Frost was born in 1902 and graduated from the U.S. Naval Academy in 1926. Frost, like the other early Directors, had seen war firsthand and had been awarded the Bronze Medal and two Silver Stars.

Frost brought a wealth of experience in communications both at sea and in staff positions to his brief tenure as Director. After a dispute with the Pentagon, he stepped down as Director in June of 1962, three months before one of the most harrowing and dangerous moments in NSA and U.S. history.

Lieutenant General Blake

Air Force Lieutenant General Gordon A. Blake replaced Frost. Like the previous occupants of his office, Blake was no stranger to combat. Blake gained valuable experience during World War II in operations communications and later in the field of research and development. His experience eventually led to his appointment as Commander of the Air Force Security Service. Blake's wartime and service pedigree were valuable assets in his role as NSA Director. Shortly after he assumed the post, he would have to draw on every bit of his talents and experiences to assist the Nation in dealing with the harrowing series of events that would come to be known as the Cuban Missile Crisis.

The Cuban Missile Crisis

In the autumn of 1962, the United States faced its most serious crisis of the Cold War.

LEADERSHIP

DIRECTORS

VADM Laurence H. Frost, USN (November 60 – June 62)

Lt Gen Gordon A. Blake, USAF (July 62 – June 65)

LTG Marshall S. Carter, USA (June 65 – August 69)

DEPUTY DIRECTORS

Dr. Louis W. Tordella (August 1958 – April 1974)

The crisis had its beginnings in Fidel Castro's Cuban Revolution. Castro's revolution initially drew strong support from all levels of Cuban society. However, by the summer of 1958, he had denounced the United States and established diplomatic relations with the communist world. Castro's move to the left prompted President Eisenhower to set the Central Intelligence Agency (CIA) to work at putting an end to Castro's reign. By the time President Kennedy occupied the Oval Office, plans to overthrow the Castro regime were fully in place. A CIA-sponsored invasion of the island was planned near the coastal town of Trinidad. Kennedy moved it to the less conspicuous location of Playa Giron, or the Bay of Pigs.

On April 17, 1961, approximately 1,300 members of a CIA-supported counter-revolutionary Cuban exile force stormed the beach. Despite assurances that their effort would foster a counterrevolution that would rally the Cuban people to their cause, the force was quickly defeated by Cuban forces and forced to surrender.

The disaster at the Bay of Pigs had huge ramifications well beyond the events of the operation. Wanting to ensure the viability of his revolution, Castro sought even closer ties with Moscow, which Moscow reciprocated. Russia was fearful of America's attempts to encircle the USSR. The United States had placed nuclear weapons in Turkey, and Premier Nikita Khrushchev saw an opportunity to give the Americans some of their own medicine by installing offensive nuclear weapons in Cuba.

But Khrushchev realized he would have to get the weapons on the island and operational before the U.S. knew what was happening.

On the morning of October 16, President John F. Kennedy was informed, through defector debriefings and U-2 photographs, that the CIA had discovered the Soviet Union was preparing to install nuclear-tipped SA-2 missiles in Cuba. Once installed, these missiles had the range to hit almost every major American city.

Due to effective denial and deception work, the Soviets were able to keep their activities secret; SIGINT had not been able to provide any advance warning of the attempted installation of these missiles.

To provide timely intelligence to a wider range of consumers, including The White House, NSA sought new, innovative ways to expand collection capabilities so that the intelligence derived was the most up-to-date possible. To achieve this, collection specialists worked with the Naval Security Group, the Navy's cryptologic organization, to develop concepts of operation for Technical Research Ships. During the crisis, ships such as the USS *Oxford* reinforced the worth of the concept.

On October 21, due largely to the work of the *Oxford*, NSA analysts were able to conclude that the Soviets had assumed control of Cuba's air defense network. The stakes were raised even higher.

During this trying time, NSA worked overtime to keep the Executive Branch informed. The White House Situation Room was reorganized to receive SIGINT product directly rather than through intermediary organizations. An NSA employee was assigned to The White House Situation Room and became a major figure in White House operations, even facilitating decision making. In addition, occasionally NSA Director Blake personally carried NSA's classified information to The White House.

Despite the fact that Kennedy controlled a wide range of nuclear weapons, hundreds of ships and an even greater number of men and equipment, he was unable to discern the mind of his counterpart, Nikita Khrushchev. What were his goals? Were the missiles a negotiating ploy, or were the Russians really willing to start a war to protect Cuba?

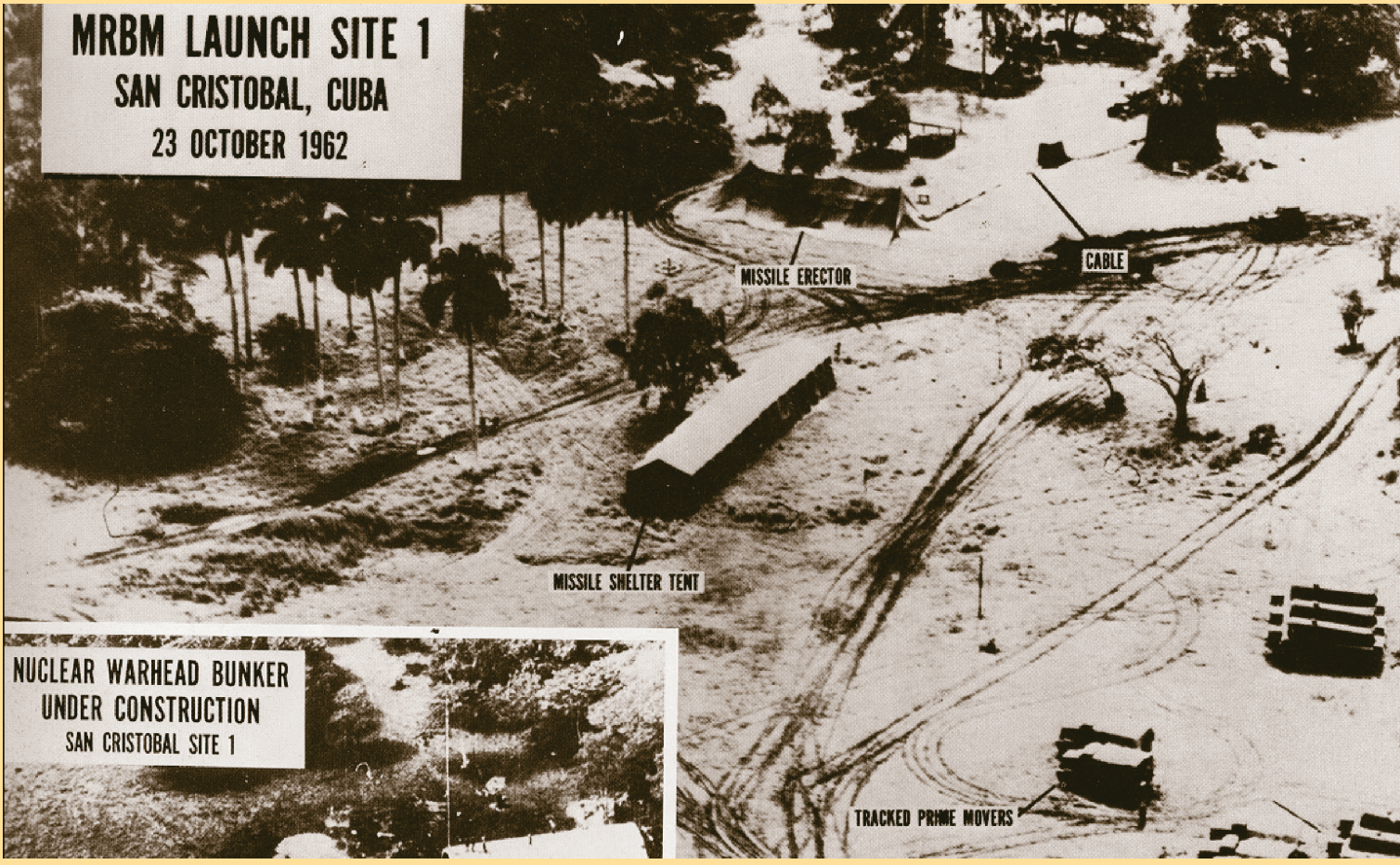
Without knowing what was happening around the world, Kennedy faced the potential of a catastrophic nuclear exchange. As the threat of Russian missiles became clearer, many of Kennedy's advisors began to lobby for an all-out invasion of the island before it was too late.

Despite the pressure from some of his most trusted advisors, Kennedy would eventually demur from the invasion option and choose another route.

On October 22, President Kennedy appeared on television and announced the U-2 findings to an anxious public. Despite assurances from the Soviet Government that the buildup was defensive, medium-range and intermediate-range ballistic missiles had been introduced into Cuba. He called for their withdrawal or destruction and established a naval "quarantine" of Cuban ports to prevent additional Soviet armaments. Kennedy also warned that further actions might be needed if the buildup of offensive weapons continued.

As the crisis moved toward a critical point, SIGINT collectors listened to the radio messages to and from the Soviet vessels on their way to Cuba. Would they turn around, or would they challenge the U.S. Navy quarantine? Any potential conflict between American and Russian ships had the potential to escalate into a wider war between the two superpowers.

Scholars differ as to when Kennedy learned that the Russian ships would not challenge the quarantine line. However, there is no doubt that U.S. SIGINT was the source. A Navy SIGINT direction finding net in the Atlantic located the Soviet ships by intercepting and triangulating messages that the ships were sending back to the Soviet Union. Some of the Russian ships were stopped dead in the water, outside the ring of American naval vessels waiting for them. Others had turned for home even earlier. By 0930 on October 24, SIGINT had determined that the Russian ship *Kimovsk* had turned around and was heading away from Cuba. By noon on the same day, it was clear from information provided by NSA and its partners that the Russians were no more anxious to start a nuclear war over Cuba than were the Americans. A confrontation had been averted, one that might have precipitated war. The President, his Cabinet, and the American people could breathe a little easier.



Soviet Strategic Missile sites under construction in Cuba, 1962.

It would be wrong to say that NSA and its partners saved the world from destruction; however, it is clear that during one of the most perilous moments in the history of mankind, the leader of the free world was provided information that led him to make prudent decisions that kept the peace, not just for America, but for the world.

Communications Intelligence

From their experiences during the crisis, NSA leaders knew that communications intelligence (COMINT) needed to be distributed faster and more widely. Over the next decade, they developed and implemented procedural and technical improvements to enhance support to intelligence consumers.

In NSA's earliest days, COMINT reports greatly resembled those of the prewar and wartime eras. Most were straight translations of decrypted intercepts. Often, reports consisted of nothing more than a 3x5 card with a typed verbatim text sent through an interagency mail system.

By 1962, at the time of the Cuban Missile Crisis, a few NSA offices had converted to electrical distribution, releasing reports via a machine that resembled a teletype. The Cuban Office, at least, also issued summary reports, compilations of many reports consolidated for ease of reading.

The experience of the missile crisis made it clear to all offices that the future was in rapid dissemination of reports. Over the next decade, although some bulkier products were still released only in hard copy, systems were installed and expanded for more timely and widespread release of reports. The new style reports were known as "Electrigrams" or "EGRAMs" for short.

USS Oxford, a Navy COMINT collection vessel during the Cuban Missile Crisis.

Gradually, NSA began to release analysis of its intercept. Some other intelligence agencies continued to insist that the COMINT system should issue only translations of intercept, leaving analysis to them. Over time, as COMINT production became more sophisticated and new sources opened up, it became evident that NSA analysts were best equipped to manage and analyze their own product.

Tides and Hurricanes

Winston Churchill once cautioned that one should "never believe that any war will be smooth and easy or that anyone who embarks on the strange voyage can measure the tides and hurricanes he will encounter..." To this day, individuals debate whether the Vietnam War was a noble cause or a horrible mistake. But from a cryptologic perspective, the war that raged in Indochina from the early sixties until the mid-seventies was a time of supreme service and sacrifice.

In the end, as was the case with much of America's involvement in the conflict, the results of NSA's cryptologic efforts to try to solve the riddle of Indochina were decidedly mixed.

As early as 1961, the Director of NSA ordered reviews of existing activities and contingency plans for Vietnam and neighboring countries. NSA responded to military requests for COMINT support by recommending limited, mobile collection in Vietnam, with an emphasis on Direction Finding (DF), including some training of the South Vietnamese in DF techniques.

The Army Security Agency (ASA), at the request of a high-level intelligence board, became the lead agency for SIGINT support in Vietnam. The first ASA troops arrived at Tan Son Nhut Air Base in May 1961 and began operations. NSA initially sent technical personnel to Vietnam for temporary duty and first assigned a permanent

Courtesy of John F. Kennedy Presidential Library

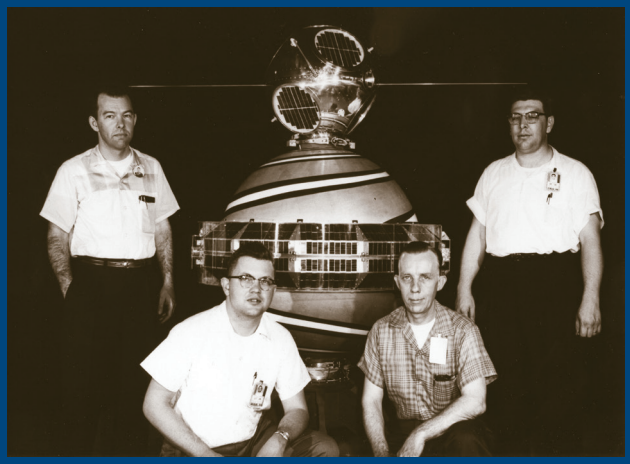
NSA provided vital information to President Kennedy during the perilous days of the Cuban Missile Crisis.

Satellite Collection

As technology and methods advanced, NSA senior technical personnel realized that information could also be collected from satellites. The collection and analysis of that information was referred to as electronic intelligence (ELINT). Collection from satellites focused on electronic signals from radars in the Soviet Union, and NSA joined the Air Force in analyzing ELINT signals. By the mid 1960s, the Agency was directly involved in the analysis of intercept from overhead collection, as well as the tasking of this increasingly valuable source.

As would be expected, other intelligence agencies wanted to be players in satellite collection, analysis and production, but they had conflicting priorities. These differences were eventually resolved, resulting in a collaborative approach to satellite tasking and analysis.

The Nation's first electronics signals satellite, GRAB (Galactic Radiation and Background), was developed by the Naval Research Lab (NRL) and was followed by a series of U.S. intelligence satellites given the code name POPPY. The National Reconnaissance Office (NRO) took over the operation of the POPPY program in 1962, shortly before the program's first satellite launch. ■



NRL team at Cape Canaveral for spin test of GRAB1 atop Transit 2A. (Left to Right) Martin J. Votaw, George G. Kronmiller, Alfred R. Conover and Roy A. Harding

representative to Saigon in April 1962. Tragically, the first soldier killed in combat in Vietnam was Specialist James Davis, an advisor to a South Vietnamese Radio Research unit.

As each of the services deployed its own SIGINT assets to provide support in the war, NSA worked with the command structure in Saigon to provide central direction and coordination of the efforts. This was not entirely welcomed at the Military Assistance Group in Saigon. Senior military leaders were apprehensive about questions of control for such an important asset as SIGINT. In Vietnam, NSA set up a number of SIGINT Support Groups (SSGs) with a mission that was expanded beyond that of previous wars. The SSGs provided and explained SIGINT to commanders, helped incorporate SIGINT with other kinds of intelligence, and relayed local requirements to SIGINT producers. This "one-stop" concept proved invaluable for military commanders' needs.

America's early involvement in Indochina was initially somewhat limited. While it considered Vietnam an area of interest, as late as November 1963 the Kennedy administration had no firm plans on the future of the operation.

After Kennedy's death, however, President Lyndon Baines Johnson decided that Vietnam was a war that needed to be won. Over time, Johnson escalated the number of troops and resources devoted to the conflict to unprecedented levels. One of the critical events that led Johnson to this conclusion occurred in the summer of 1964 off the coast of Vietnam, and NSA played a major role.

Gulf of Tonkin

On August 1, 1964, the USS *Maddox*, a destroyer patrolling the Gulf, was attacked by North Vietnamese torpedo boats in the vicinity of the Gulf of Tonkin. Due to some excellent communications-related intelligence that warned the ship about the impending waterborne assault, the *Maddox* was able to successfully repel the attack.

In response to the incident, President Johnson publicly warned North Vietnam of serious consequences should there be a repeat of the incident. On the night of August 4, 1964, the *Maddox* and a companion vessel, the USS *Turner Joy*, reported a possible second attack, although local confirmation of North Vietnamese activity was inconclusive.

While the administration was deliberating its response, they received COMINT reports from a field site and later NSA, both seeming to confirm a second attack. Unfortunately, both reports were mistranslations. When the first intercepted North Vietnamese reports came in regarding the incident, they were assumed to be describing a second attack on August 4; in reality, they were actually North Vietnamese after-action messages related to the original attack on August 1.

This false information would not be recognized for months, and the lapse in time would prove to be critical because the alleged confirmation of a second attack prompted the Johnson administration to swiftly order retaliatory bombing of North Vietnamese facilities. In addition, the incident convinced the administration that new congressional authorization for military action in Southeast Asia was warranted.

In the end, it turned out that the Gulf of Tonkin incident had been a minor incident; however, the event would have major ramifications as it gave the Johnson administration good reason to forge ahead with its plans for Vietnam.

As the United States increased it efforts in the region, NSA and its partners provided critical intelligence on the enemy and protected the critical information of the United States Armed Forces from its adversaries. By the mid-1960s, a vast network of listening posts had been established. These units' work provided the units in the field the information they needed to conduct their respective missions. (See Documents B1 & B2 at end of chapter.)

The first Soldier killed in combat in Vietnam was Specialist James Davis, an advisor to a South Vietnamese Radio Research unit.

COMSEC and Purple Dragon

American cryptologic efforts on the protect side of the equation were not as successful. The attitude that the North was a primitive culture with little in the way of cryptologic talent and resources led to complacency and overconfidence regarding U.S. efforts to protect critical information on the air waves. In the mid-1960s, NSA analysts could demonstrate from intercepted sources that the North Vietnamese were able to provide advance warning of U.S. bombing missions over North Vietnam (a program known as ROLLING THUNDER).

When the United States captured a North Vietnamese intercept site near Saigon, NSA confirmed that North Vietnam heavily relied on SIGINT as an intelligence source. This discovery was significant. NSA analysts briefed

the Joint Chiefs of Staff and components of the Intelligence Community on this development and its implications.

In response, the Defense Intelligence Agency (DIA) convened an interagency taskforce in the Pacific to identify remediation measures that could be taken to address security weaknesses and vulnerabilities. Eventually, this DIA-led group was known by the covername PURPLE DRAGON.

After the PURPLE DRAGON group completed its review, the blame for the breaches in security surrounding ROLLING THUNDER missions was placed on poor communications security (COMSEC) practices by U.S. forces, compounded by operational practices that made bombing raids predictable. The study group made a number of recommendations to correct the problems. The findings of the PURPLE DRAGON team were partially implemented and gave rise to the discipline of Operations Security (OPSEC), which is still used today.

As the Nixon administration adopted the policy of "Vietnamization" of the war, NSA helped in the transfer of equipment and provision of training to a South Vietnamese intelligence organization.

The Nation's experience in Vietnam will be debated for years to come. But no one should ever forget the countless acts of courage and bravery demonstrated not only by our Nation's war fighters, but also by the silent sentinels of the cryptologic service.

U.S. Army Signal Corps Communications on Monkey Mountain, Vietnam.

The *Liberty*

In 1967 tensions were once again rising in the Middle East between Israel and her Arab neighbors. Hoping to collect critical intelligence in the region, the USS *Liberty* was sent to the eastern Mediterranean. The ship, manned by a full complement of Navy SIGINT personnel and three NSA civilians, went on station four days into the Six-Day War.

U.S. Navy ships were ordered to draw back at least 100 miles from the area of operation; however, due to a host of errors, the *Liberty* did not get the message. On the afternoon of June 8, off the coast of the Sinai Peninsula, the ship was attacked by Israeli Navy and Air Defense Forces.

Thirty-four crew members were killed and 171 wounded, and the ship itself was badly damaged. Commander William McGonagle, the ship's captain, despite being wounded, was able to direct a robust salvage operation that somehow managed to keep the ship afloat. For his bravery, heroism, and actions in saving the ship and administering to his crew, McGonagle would later be awarded the Medal of Honor.

Eventually, the Israeli Government apologized for the incident and attributed it to a series of errors. In addition, Israel agreed to pay compensation to the United States. After an investigation, the U.S. ultimately accepted the apology. To this day, historians continue to debate the exact nature of events that transpired, and intense controversy remains over whether or not the attack was deliberate.

Despite the controversy, what can be said unequivocally is that the crew's service and sacrifice exemplified the best traits of the U.S. Navy and the cryptologic service, and demonstrated once again that the discipline can sometimes be a dangerous one. (More information on the USS *Liberty* can be found on NSA.gov.)

The *Pueblo*

Six months after the *Liberty* incident, another distressing incident, involving the USS *Pueblo,* occurred. In 1967 North Korean aggression

The Ears of Neptune

The critical work of the USS *Oxford* during the Cuban missile crisis prompted the "powers that be" in the community to expand the program of U.S. Navy ships collecting critical SIGINT.

Like U.S. Navy ships everywhere, cryptologic vessels like the *Oxford* were a flexible asset that could be deployed on short notice and sent to any coastal location to gather pertinent and real-time intelligence.

But, while these technical research ships were indeed versatile and manned by crews of talented and dedicated men, they also proved to be exceedingly vulnerable. This vulnerability led to two tragic incidents at sea involving the USS *Liberty* in 1967 and the USS *Pueblo* in 1968. These experiences exposed the problems in the use of these ships and ultimately led to the program's termination by the end of the decade. ■

The USS Liberty in drydock, Malta 1967.

against South Korea increased markedly. Needing to know more about the events in the region, the U.S. Navy deployed the USS *Pueblo* to collect critical information off the North Korean coast. On January 28, 1968, while the *Pueblo* was in international waters, North Korean patrol boats attacked and overwhelmed the lightly defended ship.

During the capture of the vessel, one crew member was killed. The remaining 83 crew members, including the ship's captain, LCDR Lloyd Bucher, were captured and taken to North Korea where they were harshly interrogated and brutally tortured. After a long series of negotiations, the United States agreed to sign a "confession" claiming that the ship had violated North Korean waters, and the crew's year-long captivity finally came to an end. However, while Bucher had managed to bring all but one of his crew back safely, copious amounts of both sensitive and precious cryptomaterials had fallen into the hands of the North Koreans.

It is worth noting that NSA's role in the *Pueblo* case was mainly as a technical advisor. The Agency, as part of the wider Intelligence Community, was asked for its advice on the mission itself, which had been deemed dangerous by several experts and organizations. In the end, NSA decided to approve the mission, but also forwarded a warning statement prior to the vessel's deployment about the growing aggressiveness of North Korea. Despite the warnings and concerns, the mission went forward.

Change of Command

The 1960s were challenging times for both NSA and the Nation. Events like the Cuban Missile Crisis demonstrated that policymakers and generals needed information that was both accurate and timely, and the Agency took a number of steps to increase its efficiency and operations.

Lieutenant General Carter

In the spring of 1965, General Blake retired and was succeeded by one of his West Point classmates, Lieutenant General Marshall S. Carter, USA. General Carter had extensive experience in the realm of civil affairs and intelligence, serving as General Marshall's executive assistant and as Deputy Director at CIA. His broad experience helped to shape his vision for dealing with NSA's emerging role in the Intelligence Community.

Watchmen on the Walls of Freedom

On the day of his untimely death, President John F. Kennedy planned to give a speech in Dallas that would focus on the fact that America and Americans were "Watchmen on the Walls of Freedom." It was in this same spirit in the 1960s that NSA began to develop a series of watch centers to ensure that the United States could better respond to the grave challenges of the Cold War.

NSOC

The crises of the late 1960s led directly to the establishment of the National SIGINT Operations Center (NSOC). Efforts had been made to consolidate the huge volume of traffic into a central location to enhance the ability of NSA to provide accurate and timely intelligence. NSOC was a significant step forward in accomplishing this goal.

The multinational character of the crises of the 1960s prompted Agency leadership to organize along geographic lines. This structure meant that the wars and subsequent tensions in the Middle East, the Soviet invasion of Czechoslovakia, and the capture of the USS *Pueblo* would be handled by employees in different offices. The events of the 1960s demonstrated to NSA leaders the need for immediate input from several offices to get a full understanding of what was happening around the globe.

To achieve this goal, the National SIGINT Watch Center was created in December 1968. Ironically, while the proposal was being considered, a major crisis occurred -- the shootdown of a U.S. Navy EC-121 SIGINT reconnaissance aircraft by North Korea in April 1969. As was typical for that time, information for crisis management for this incident went to several watch centers at NSA, with no central repository, compounding the difficulty of collating the intelligence. This incident clearly demonstrated the need for change, and

the concept of a centralized watch center for the Agency was approved.

A general outline for a National SIGINT Watch Center was prepared by September, but delays occurred. Turf battles erupted over the loss of individual watch centers. Finally, in 1972, after several delays, a formal location was identified. The Center began limited operations in December of that year and a few months later on February 21, 1973, was formally inaugurated as the National SIGINT Operations Center (NSOC).

Eventually, NSOC was able to assume a wide range of functions in NSA's daily operations and quickly became the focal point for crisis response at NSA until Operation DESERT SHIELD in the early 1990s, when the practice of convening special cells tailored to particular crises became standard. NSOC is known as the "Nerve Center of NSA" and was renamed to the National Security Operations Center in 1996.

DEFSMAC

Many Americans feared that the USSR was much more advanced than the United States in development of intercontinental missiles. This was not true; however, there was a growing threat from a wide range of Soviet weapons systems. The threat became even more apparent after the Cuban Missile Crisis of October 1962.

In January 1963, NSA consolidated existing warning facilities into the Space and Missile Analysis Center (SMAC). Later in the year, the Agency joined with the Defense Intelligence Agency (DIA) to consolidate this facility with other Defense Department components in the missile warning business.

From this innovative consolidation, a new organization emerged – the Defense Special Missile and Astronautics Center (DEFSMAC). Today, DEFSMAC is a leader in weapons and space intelligence. Over the last half century, this vital organization has had an NSA senior official as chief and a deputy chief from DIA. It remains headquartered at NSA's Fort Meade complex.

The Travis Trophy

In 1963 a worker at Arlington Hall Station, home to the Army Security Agency and some elements of NSA, found a trophy on a shelf in a storeroom, which was brought to the attention of the Director, Lt Gen Blake.

The trophy had been given to the United States in 1948 by Sir Edward Travis, Director of Britain's Government Communications Headquarters (GCHQ). Travis proposed that it be awarded to the winner of a complicated sports competition between the Army and Navy cryptologic organizations. The trophy was awarded to the Army after a tournament that involved games of tennis, golf, and chess. As far as is known, there was not another such competition after 1948.

After the discovery of the trophy in 1963, General Blake consulted with the Director of GCHQ, and, with his concurrence, designated the loving cup as an annual award to the U.S. cryptologic field station that had made the year's most significant contribution to operations, management, or administration in cryptology. Though later joined by other competitions and awards, the Travis Trophy became the most prestigious award in the cryptologic community and still holds that position today. ■

In 1964, the first winner of the Travis Trophy was the 6988th Security Squadron in Yokota, Japan.

The Enterprise Expands

After the first building constructed in the mid-1950s proved inadequate for NSA's growing workforce, the Agency constructed an adjacent, nine-story structure, which opened in 1963. Offices at the newly-configured campus focused primarily on the COMINT function. The Director located his office on the top floor, and the workers began to refer to the building as the "Headquarters Building," with its "Ninth Floor" synonymous for the Agency's leadership.

Things were changing on the protect side as well. In 1968 the Communications Security organization also opened a new building in the NSA complex. While the two buildings were on the same campus, the COMSEC organization was some distance away from the main complex.

The crises of the 1960s and, more particularly, the war in Vietnam, necessitated rethinking COMSEC doctrine and equipment. In response, NSA developed the KW-7 device to encrypt tactical message traffic in combat.

A series of devices was developed to protect communications during the Vietnam War. The original cipher machine, the KY-8, was generally viewed by the military as too heavy and too slow for use in combat. Later versions, such as the KY-28 and KY-38, took advantage of newer technology with integrated circuits, making them more portable, but still secure.

The National Cryptologic School (NCS)

While buildings and technology are important, the need to train employees in effective cryptologic methods is vital to NSA's mission. Each step in the cryptologic process is

LTG Marshall S. Carter, USA, Director NSA, observes class in progress during a 1967 visit.

The NSA Headquarters Building, a nine-story structure, opened in 1963.

specialized and technical and requires unique training to enable employees to operate at high professional levels. One of the most important organizations in achieving this goal is the National Cryptologic School.

Employee training has been part of U.S. cryptology since NSA's 20th century inception. In the beginning, much of what passed as training was the result of on-the-job mentoring, but over time Agency leaders began to realize that organized classes were also needed.

The role of NCS grew as NSA's hiring increased in the 1960s. More new employees came to the Agency from universities and lacked military cryptologic experience that had been typical in the past. More and more, Agency operations required specific technical knowledge that could not be found anywhere other than within the walls of the Agency.

With this in mind, NSA tailored its in-house professional training and education program, and, in April 1965, the Department of Defense founded the National Cryptologic School via DoD Directive 5100.47. Since that time, the institution has served as the cryptologic training ground for both military and civilian members of the workforce.

In 1965, the NCS superintendent title changed to commandant to more accurately reflect the authority vested in the position and the organization. The Cryptologic School or "The Schoolhouse" – as it was popularly known among the workforce – grew in scope and importance, and in 1972, it was given additional responsibility for training throughout the cryptologic community, including the Service Cryptologic Agencies. Today the NCS continues to meet the training challenges through its many well-respected training programs and educational opportunities.

More Speed in Smaller Boxes

Early on, NSA recognized computing as a cornerstone of modern cryptologic operations

and took strong measures to become a leader in the field. The Agency invested aggressively, emphasizing computer purchase requirements in its budget. Some advanced models were procured and others were developed by the Agency's research component. NSA also worked with outside sources to develop specific- and general-purpose computers. The goal was to get the Agency as close to the borders of the technological frontier as quickly as possible.

Evidence of NSA's pursuit of computerization is the fact that the Agency was an early adopter of the UNIVAC. Purchased in 1963, this system had the capacity to handle a large volume of communications from remote stations simultaneously.

During this period, NSA technicians constantly sought solutions and developed advanced programs for receiving and distributing communications intercept, as well as for storing large amounts of data.

The result of this corporate effort was that by the end of the 1960s, NSA could boast that it had over 100 computers, covering five acres of floor space, serving both defense and national SIGINT and COMSEC customers. ■

UNIVAC system purchased by NSA in 1963.

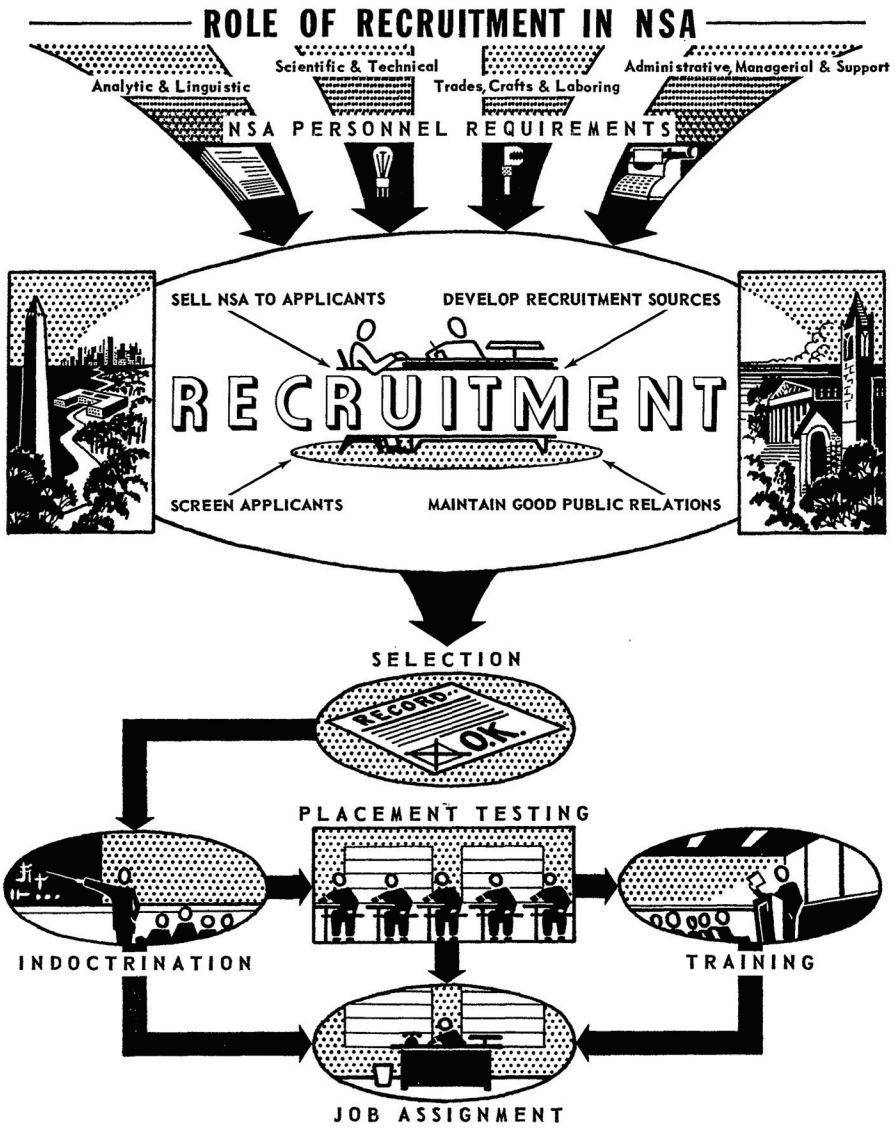
National Security Agency
Historic Documents

Document A – Two excerpts from the Recruiters Manual: Interviewing and Recruiting for NSA, December 1960

Document B – Two messages in response to the Gulf of Tonkin Incident, August 1964

DOCID: 3978541

FOR OFFICIAL USE ONLY



Document A-1: The outline of the recruitment interview pattern from the Recruiters Manual.

DOCID: 3978541

SECTION 3

GENERAL INSTRUCTIONS FOR CONDUCTING
THE RECRUITMENT INTERVIEW

The major steps in the interview pattern which each recruiter should follow in conducting a recruitment interview are outlined below. The outline is followed by a brief explanation of each step. When conducting an interview, the recruiter should introduce each step in the same sequence as it appears in the outline.

Outline of the Recruitment Interview Pattern

1. Introduce yourself and exchange pleasantries.
2. Obtain the identifying data called for on the front of the Recruiter's Interview Record.
3. Explain the interview pattern to the applicant.
4. Explain the Agency's security clearance procedure.*
5. Ask the applicant questions.*
6. Permit the applicant to ask questions.*
7. Provide additional information about NSA.
   a. Agency's mission.
   b. Work interests relevant to the occupational fields for which the applicant appears to qualify.
   c. Training Program (if applicable).
   d. Cooperative Education Program (if applicable).
   e. Desirable features of employment with NSA.
   f. Undesirable features of employment.
8. Explain how to apply for employment

* The interview can be terminated at this stage if it seems desirable to do so.

~~FOR OFFICIAL USE ONLY~~

Document A-2

INCOMING MESSAGE

THE JOINT CHIEFS OF STAFF

~~SECRET~~

PRECEDENCE (ACTION)	PRECEDENCE (INFO)
FLASH	FLASH

184

Z 071101Z

FM CINCPACFLT

TO RUHLHQ/CINCPAC

INFO RUEKDA/JCS
RUECW/CNO

DECLASSIFIED
Authority E.O. 11652 SEC. 5(A) and (D)
By JB, NARS, Date 4-28-76

~~S E C R E~~ T

PROOF OF ATTACK (U)

A. JCS 7770 DTG 061642Z NOTAL

B. CINCPAC 061840Z NOTAL

1. IAW REF B, FOLLOWING INFO IS SUBMITTED FOR RESPONSE TO REF A:

A. USS MADDOX (DD 731), WHILE ON PATROL IN THE GULF ON TONKIN, WAS ATTACKED AT 1508 GOLF ON 2 AUGUST BY THREE NORTH VIETNAMESE MOTOR TORPEDO BOATS. MADDOX WAS, AT THE TIME OF ATTACK, APPROXIMATELY 30 MILES FROM THE NEAREST LAND. DURING THIS UNPROVIKED ATTACK, THREE TORPEDOES WERE FIRED AT MADDOX. ALTHOUTH NO TORPEDOES HIT MADDOX, ONE MACHINE GUN BULLET WAS OBSERVED HITTING THE SHIP. THIS BULLET WAS SUBSEQUENTLY REMOVED FROM THE AMMUNITION MAGAZINE IN WHICH IT HAD LODGED AND WILL BE RETURNED TO THE UNITED STATES AS EVIDENCE. MADDOX FIRED HER GUNES IN SELF DEFENSE AND WAS ABLE TO REPULSE THE ATTACKERS. MADDOX PROBABLY SANK ONE PT IN THIS ENGAGEMENT. THIS ATTACK HAS BEEN ACKNOWLEDGED BY THE NORTH VIETNAMESE.

B. AFTER THIS ATTACK, MADDOX REFUELED AND RETURNED TO THE PATROL IN THE GULF OF TONKIN IN COMPANY WITH USS TURNER JOY (DD 951). AT ABOUT 2108 GOLF ON 4 AUGUST, HEN MADDOX AND TURNER JOY WERE ON A SOUTHEASTERLY COURSE APPROXIMATELY 60 MILES FROM THE NORTH VIETNAMESE COAST, THREE HIGH SPEED RADAR CONTACTS WERE DETECTED ABOUT 14 MILES TO THE EASTWARD OF THE TWO SHIPS. AT 2119 GOLF THE CONTACTS, WHICH WERE DESPLAYED ON THE RADAR SCREENS OF BOTH SHIPS, INDICATED PROBABLE

INFO.....CJCS-2 DJS-3 SJCS-1 J3-6 DIA-1 NMCC-2 CSA-2 CSAF-2 (CMC)-2
(WHITE HOUSE)-3 FILE-1 (25) SO (STATE) (CIA) (NSA)

REF B NOT HELD, WILL FURNISH ON REQUEST IF OBTAINABLE

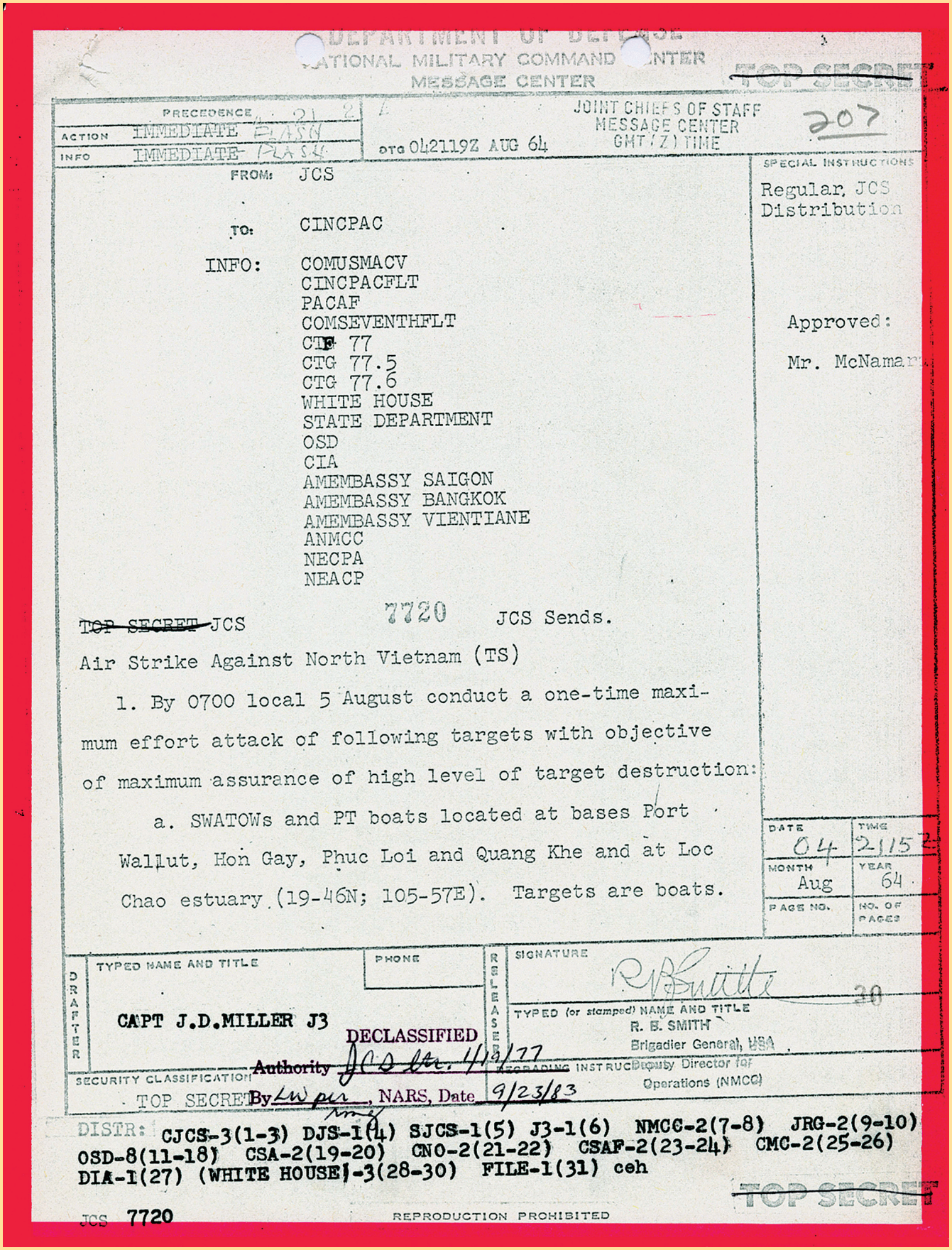
DUTY OFFICER		PAGE OF PAGES		MESSAGE IDENTIFICATION	
				CITE NO.	DTG
WU/JBE	KLH	1	3		071101Z AUG 64

JCS FORM NO 1 DEC 63 58

REPRODUCTION PROHIBITED

~~SECRET~~

Document B-1: Above and opposite page, messages from the Joint Chiefs of Staff in response to the Gulf of Tonkin Incident in August 1964. (Lyndon Baines Johnson Library and Museum)



DEPARTMENT OF DEFENSE
NATIONAL MILITARY COMMAND CENTER
MESSAGE CENTER

~~TOP SECRET~~

PRECEDENCE 21 2
ACTION IMMEDIATE FLASH
INFO IMMEDIATE FLASH

DTG 042119Z AUG 64

JOINT CHIEFS OF STAFF
MESSAGE CENTER
GMT (Z) TIME

207

FROM: JCS

TO: CINCPAC

INFO: COMUSMACV
CINCPACFLT
PACAF
COMSEVENTHFLT
CTF 77
CTG 77.5
CTG 77.6
WHITE HOUSE
STATE DEPARTMENT
OSD
CIA
AMEMBASSY SAIGON
AMEMBASSY BANGKOK
AMEMBASSY VIENTIANE
ANMCC
NECPA
NEACP

SPECIAL INSTRUCTIONS
Regular JCS Distribution

Approved:

Mr. McNamara

~~TOP SECRET~~ JCS 7720 JCS Sends.

Air Strike Against North Vietnam (TS)

1. By 0700 local 5 August conduct a one-time maximum effort attack of following targets with objective of maximum assurance of high level of target destruction:

a. SWATOWs and PT boats located at bases Port Wallut, Hon Gay, Phuc Loi and Quang Khe and at Loc Chao estuary (19-46N; 105-57E). Targets are boats.

DATE	TIME
04	2115Z
MONTH	YEAR
Aug	64
PAGE NO.	NO. OF PAGES

DRAFTER
TYPED NAME AND TITLE: CAPT J.D.MILLER J3
PHONE

RELEASER
SIGNATURE: R B Smith 30
TYPED (or stamped) NAME AND TITLE: R. B. SMITH, Brigadier General, USA, Deputy Director for Operations (NMCC)

DECLASSIFIED
Authority JCS ltr. 4/19/77
By LW per rmg, NARS, Date 9/23/83

SECURITY CLASSIFICATION: TOP SECRET
REGRADING INSTRUCTIONS

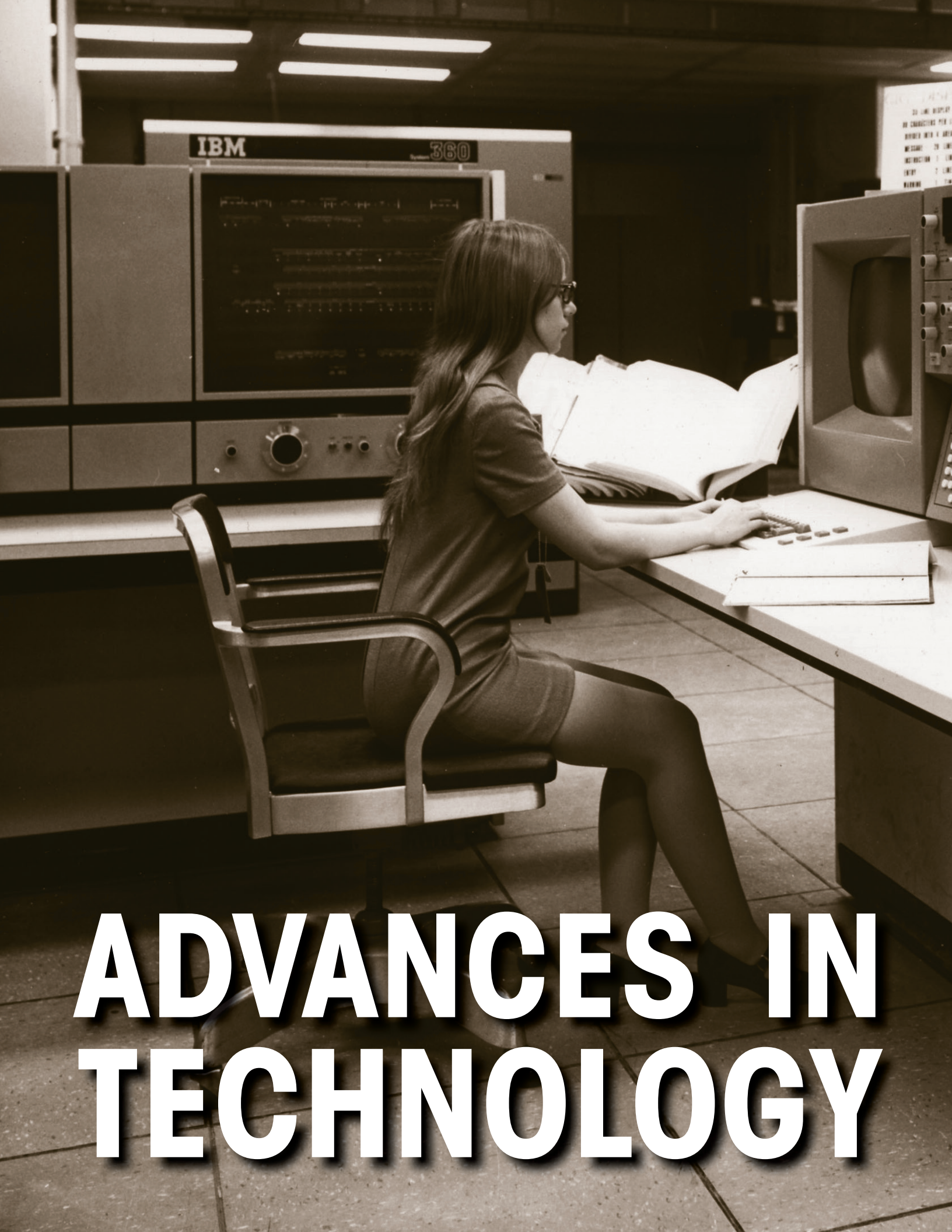
DISTR: CJCS-3(1-3) DJS-1(4) SJCS-1(5) J3-1(6) NMCC-2(7-8) JRG-2(9-10) OSD-8(11-18) CSA-2(19-20) CNO-2(21-22) CSAF-2(23-24) CMC-2(25-26) DIA-1(27) (WHITE HOUSE)-3(28-30) FILE-1(31) ceh

~~TOP SECRET~~

JCS 7720

REPRODUCTION PROHIBITED

Document B-2



ADVANCES IN TECHNOLOGY

1970s

As the 1970s dawned, thousands of American servicemen continued to fight and die in Vietnam. While both the Soviet Union and the United States appeared to be far more cautious regarding nuclear war than in previous decades, the issues that had brought the Cold War to fruition were far from being settled. In addition, the ever-present tensions in the Middle East continued to simmer.

During this time, the Soviet Union and its allies continued to be NSA's major concern. Cold War intelligence targets included Russian military forces, strategic rocket forces, air defense forces, and airborne troops. In addition, commanders also sought intelligence on the other countries of the Warsaw Pact, including Bulgaria, Czechoslovakia, East Germany, Hungary, Poland, and Romania.

At the same time, technology continued to advance to unprecedented levels. Although the information revolution was decades away, the '70s would see a number of technological advances that would prove to be key to the Agency and its mission.

The decade brought America some unique challenges, including many in which NSA would play a major role.

Vice Admiral Gayler

In the late summer of 1969, General Carter retired from active duty. Although his replacement, Vice Admiral Noel Gayler, USN, had little intelligence experience, he had distinguished himself in combat in WWII and was the first U.S. Navy pilot to win three Navy Crosses.

By the mid-1970s, NSA was moving toward desktop terminals and away from supercomputers like the one shown here.

Gaylor relied heavily on his military experience during the formation of the Central Security Service (CSS), one of his major accomplishments as Director.

Louis W. Tordella, Ph.D.

Born in Garrett, Indiana, Lou Tordella showed an uncanny affinity for mathematics, eventually obtaining a doctoral degree in the discipline. During WWII, he served in the Navy, and after the war, he went directly into cryptologic work for the Navy's codebreaking organization, OP-20-G. Tordella stayed in the Navy until 1949, when he joined the newly created Armed Forces Security Agency (AFSA).

His ingenuity and skill brought him to the very front rank of cryptologists. He was an early advocate of the use of computers for cryptologic work and helped to cement a close working relationship with American industry. Dr. Tordella became the Deputy Director of NSA in 1958, and remained in the post until his retirement in 1974. He thus became the longest serving Deputy Director in NSA's history.

The NSA campus as it looked in 1970

The Central Security Service

Today NSA is truly a worldwide enterprise with thousands of both military and civilian workers. However, despite its presence around the globe, it cannot do its job without one of its most important partners, the Central Security Service.

Traditionally, the U.S. Intelligence Community has depended on the Soldiers, Sailors, Airmen, Marines, and Coast Guardsmen of the United States Armed Forces and their resources to collect intelligence throughout the world. However, as NSA requirements increased, it became clear that the organizations and systems used by the military to collect cryptologic intelligence needed to be updated and formalized.

In 1971 President Richard Nixon, in response to a Pentagon study, announced plans to consolidate NSA and the Service Cryptologic Agencies (SCAs) into a new unified command, with NSA absorbing SCA functions. As Director, Admiral Gayler was tasked with overseeing the consolidation designed to "provide a more unified cryptologic organization within the Department of Defense."

A year later, Secretary of Defense Melvin Laird expressed his concern that the proposed consolidation would result in NSA focusing on strategic requirements rather than the needs of tactical military commanders. Laird proposed a compromise that would assure senior military leaders that under the new arrangement they would continue to receive the required cryptologic support.

Eventually all parties involved came to terms with the concept, and in February of 1972 the CSS was established via National Security Council Intelligence Directive 6 and Department of Defense Directive 5100.20. While the proposal stopped short of establishing a combined command, it proved effective in increasing performance standards and training. Most importantly, the initiative laid the groundwork for the increased centralization of NSA and military cryptologic assets. (See Document A at end of chapter.)

LEADERSHIP

DIRECTORS

VADM Noel Gayler, USN
(August 1969 – August 1972)

Lt Gen Samuel C. Phillips, USAF
(August 1972 – August 1973)

Lt Gen Lew Allen, Jr., USAF
(August 1973 – July 1977)

VADM Bobby Ray Inman, USN
(July 1977 – March 1981)

DEPUTY DIRECTORS

Dr. Louis W. Tordella
(August 1958 – April 1974)

Benson K. Buffham
(April 1974 – April 1978)

Robert E. Drake
(May 1978 – April 1980)

The Church Committee

From its inception, NSA had developed what could only be described as a cursory relationship with the U.S. Congress. At times, the Agency would engage with Congress on budget matters and other serious issues. However, due to the secretive environment of the Cold War and the perception that the subject matter the Agency dealt with was both highly specialized and classified, many congressmen were uncomfortable exercising more than minimal oversight.

This scenario changed dramatically after credible media reports surfaced that U.S. intelligence agencies had violated the rights of American citizens by engaging in unlawful behavior. In order to investigate these claims, the United States Senate formed an investigating committee under Senator Frank Church (D, Idaho). Soon after, the House would follow suit, forming a committee under Congressman Otis Pike (D, New York). When their work was finally completed, both investigative bodies produced reports denoting that two specific NSA projects, Project SHAMROCK and Project MINARET, had violated a number of Americans' Fourth Amendment rights. ■

NSA Director, Lt Gen Lew Allen, Jr. USAF testified during a Senate hearing in 1975. (See Document B at end of chapter)

A critical part of the directive called for the Director of NSA to serve simultaneously as the Chief of the CSS. The initiative also tasked the Director to carry out a wide range of responsibilities in the areas of tasking, training, research and career development, and government cryptology.

Lieutenant General Phillips

In the early summer of 1972, Admiral Gayler gained his fourth star and headed off to Hawaii to become head of the U.S. Navy's Pacific Command. Taking his place was Air Force Lieutenant General Samuel C. Phillips. Phillips had no intelligence experience, but was well versed in the area of missiles and space. His focus during his brief time at NSA was on organizational reforms and streamlining NSA operations.

Lieutenant General Allen

He was replaced by another Air Force General, Lieutenant General Lew Allen, Jr., in August 1973. Previous to his appointment to the Directorship, Allen had managed a wide range of overhead assets, including satellites that monitored Soviet nuclear arms control treaty compliance. Allen was the first NSA Director to hold a Ph.D., having obtained his doctorate in physics at the University of Illinois.

One of his most compelling challenges was to deal with the ramifications of the investigations of the U.S. Intelligence Community, including NSA, by the Church and Pike Committees.

SHAMROCK and MINARET

In the 1930s Congress passed a law prohibiting communications companies from revealing the content of telegrams to third parties. During WWII, however, Congress implemented a series of censorship laws that superseded the original law and allowed U.S. authorities to examine the content of telegrams sent to and from the United States. In addition, any encrypted messages were sent to Arlington Hall.

When WWII ended, the authorization for the program expired. However, with the coming of

the Cold War, the Army Security Agency appealed to the patriotic sentiments of the companies to continue to provide copies of messages to and from the Soviet Union. This practice, by then known as Operation Shamrock, continued up to the NSA era.

The Church Committee raised concerns about whether NSA, in carrying out Operation SHAMROCK, had exceeded its legal authorities and violated the privacy rights of Americans as protected by the Fourth Amendment.

Operation MINARET began in the 1960s. The project involved the monitoring of the international voice communications of specific U.S. citizens whose names had been placed on a "watch list."

A Guide for the Silent Sentinel: United States Signals Intelligence Directive (USSID)

The activities of the Church and Pike Committees revealed holes in the legal procedures that underpinned NSA and its work, although, from its earliest days NSA had sought to construct standards and regulations to govern and guide its work.

The predecessor to the USSID system, dating from 1958, was the Manual of U.S. SIGINT Operations (MUSSO). MUSSO was intended to bring structure and orderly procedures to a SIGINT system that had grown rapidly over the previous decade and worked efficiently in its early years.

System managers, however, found serious difficulties with MUSSO as the cryptologic environment evolved and greater challenges emerged. Specifically, there were serious problems in trying to craft a system that could adapt to the wide range of changing procedures and practices in timely ways. Most importantly, the manual did not provide any clear authority for the procedures in question.

With the growing demand for SIGINT, it was clear that NSA needed better guidelines and, in the early 1970s, NSA's leadership introduced the United States Signals Intelligence Directive (USSID) system. Unlike previous systems, these directives provided timely procedural guidelines for practitioners throughout the SIGINT system. They could also be updated quickly to reflect changing needs and procedures and be disseminated rapidly via electrical communications.

The development and promulgation of USSID #1 proved to be critical to the Intelligence Community. Issued in 1971, the document spelled out the structure of the U.S. SIGINT System around the world. (See Document C at end of chapter.) Over time these USSIDs -- NSA directives on SIGINT -- would prove to be indispensable to NSA employees and affiliates in gaining an understanding of the proper handling of SIGINT. To ensure that all Agency employees and affiliates were familiar with the standards, training requirements on the handling of information regarding U.S. persons were stringent and demanding.

A Host of Increasing Asymmetrical Challenges

In addition to the Soviet threat, terrorism emerged as an important concern in the '70s, which sparked a significant shift in how NSA organized its operational and analytic business. Real-time reporting was essential.

Despite the challenges associated with "standing up" a new analytic area, NSA proved to be adept at producing critical information on terrorist incidents and activities. In 1974 Agency analysts uncovered a plot to assassinate Secretary of State Henry Kissinger during an overseas trip.

During the '70s, NSA became directly involved in covering terrorist-related kidnappings, assassinations, and hijackings. The support and assistance provided by the Agency in these events were ultimately seen as indispensable to the Nation's ongoing effort to prevent and manage terrorist threats. These activities further cemented NSA's key role in providing intelligence support to The White House, as well as other important consumers.

Vice Admiral Inman

In 1977 General Allen gained his fourth star and became Commander of the U.S. Air Force Systems Command. He was replaced by Vice Admiral Bobby Ray Inman, USN, the fourth Director of the '70s era. Unlike some of his predecessors, he had an impressive intelligence background. Inman served in the Korean War and had assignments as an Operations Intelligence Analyst at NSA and as Assistant Chief of Staff for Intelligence to the Commander in Chief, U.S. Pacific Fleet. His prior assignment as Vice Director, Plans, Operations and Support at DIA also gave Inman invaluable experience in the complexities of intelligence. His tenure continued to focus on the Soviet/Warsaw Pact target, although transnational targets, such as terrorism and counternarcotics, were beginning to come to the forefront. After serving as DIRNSA, VADM Inman went on to become Deputy Director and later Acting Director of the CIA.

The NESTOR system was developed in answer to the military's need for lighter and more efficient communication systems. The Soldier above is using the KY-38 "manpack."

Securing Networks

Developments in cryptographic technology boomed in the 1970s. The new public cryptography gave NSA a fresh challenge -- it had to not only keep up with, but find a way to stay ahead of the curve.

Great leaps forward in computer and electronic network technology meant NSA had to become expert in securing information systems. As newer, faster, and more efficient ways of storing and moving information developed, the private sector and scientific community grew concerned about the security of their communications. Demands for protection led to rapid developments in publicly available cryptology.

NSA struggled with this dilemma, largely because, while the Agency understood the need for robust public cryptography, its first mission was to maintain the cryptologic capabilities needed to protect the Nation. The fear was that the Nation's adversaries would be able to easily buy U.S. commercially available encryption technology.

The Agency and federal authorities realized that, while exporting the new technology was good for economic reasons, it needed to be balanced against security concerns. In sum, strong public cryptography could harden COMINT targets, and thus deny vital information to decision makers. On the other hand, if the Agency took too aggressive a stance, it would run the risk of being seen as curtailing the rights of American citizens. NSA had to proceed cautiously in its efforts to allow the free flow of commerce while at the same time doing what was needed to protect the Nation.

But while the Agency was rightfully concerned about the challenges of public cryptography, its first obligation was securing government and military communications. Drawing on its vast

expertise in the field, the Agency developed a group of cipher machines, including the first device that combined radio and encipherment in a single unit.

During this time, NSA was also developing lighter and more efficient communication systems for military use. The Vietnam War taught the Agency's system developers that troops in the field were reluctant to use communications equipment that was too heavy or cumbersome. As a result, the Agency's communications security organization began to develop equipment better suited to COMSEC in a war zone. Under the NESTOR program a number of portable devices that retained high security and good voice quality were produced.

The White House and Executive Branch

In 1976 The White House directed NSA to look for solutions that would ensure U.S. communications were secure. By that time, senior officials had begun to realize the threat posed by Soviet monitoring of communications within the United States and the vulnerability of American communication networks.

The National Security Decision Memorandum tasked NSA to work with the Office of Telecommunications Policy to develop an action plan for the express purpose of ensuring that "U.S. citizens and institutions have a reasonable expectation of privacy from foreign or domestic intercept."

The White House plan, implemented in 1977, called for expedited measures to secure communications in the Washington, New York City, and San Francisco areas. The administration considered these areas as the most vulnerable to Soviet intercept efforts. These proactive measures worked and were later extended more widely in the U.S. Preventive measures included shifting sensitive government communications from microwave to cable and bulk scrambling for microwave links (See Document D at end of chapter.). NSA's success in this arena earned it the reputation it still enjoys as the world's leader in strong communications security practices and devices.

The Mayaguez Incident

In May 1975, NSA issued a series of summary intelligence reports detailing the capture of American merchant sailors on the ship *Mayaguez* by the Khmer Rouge in Cambodia. The *Mayaguez* was a U.S. cargo ship involved in the support of U.S. forces in Southeast Asia. On May 7, 1975, the ship left Hong Kong on what was to be a routine voyage. On May 12, 1975, the *Mayaguez* was 60 miles off the coast of Cambodia when it was attacked and boarded by Khmer Rouge naval forces and forced to follow the Cambodian ships toward the mainland.

President Gerald Ford denounced the action as an "act of piracy" and demanded immediate release of the ship. Despite the attempts of the Ford administration to find a diplomatic solution, all efforts failed, and on May 14, the President ordered military action. A U.S. Marine Corps detachment in the Philippines was given the assignment and instructed to board the ship at sea.

Early in the morning of that day, the Marine contingent boarded the *Mayaguez* and took control of the vessel. Shortly after the boarding, a Thai fishing boat approached the USS *Wilson*, which was supporting the amphibious assault. Aboard the fishing boat were a Thai crew and the 39 men of the *Mayaguez*. They had been set free by their captors. By noon, all *Mayaguez* crewmen were back aboard their own ship.

Since the resolution of the incident, historians and analysts have debated the reasons for the unexpected release of the *Mayaguez* crew. Some have proposed that either China or another nation with influence over the Khmer Rouge played a role, but the complete reason will never be known.

Remote Keying

Soviet espionage activities in the United States steadily grew in the 1970s, prompting

the U.S. to develop improved voice security equipment. Despite these efforts, there were limits to what could be accomplished.

First, the limit on users for each secure telephone system in the 1960s was capped for technical reasons at about 300. This cap prevented the widespread deployment of devices throughout the Department of Defense's other government departments. In addition, existing COMSEC voice equipment was cumbersome to use and had poor voice quality –often described as "Donald Duck" quality.

For these and other compelling reasons, many officials resisted using the equipment. Their reluctance placed U.S. information and assets at risk. NSA realized that improvements were needed, and over time the voice quality of the systems greatly improved. However, the problem of limited users still remained due to both cost and technical issues.

To address this challenge, in 1967 NSA's Research and Development organization proposed the concept of a central keying facility. The proposal rested on the premise that every communication device would have a unique cryptographic key. All secure calls would be routed to a central facility that held keys for all potential users. This revolutionary concept was called BELLFIELD.

Courtesy of Gerald Ford Presidential Library

During the Mayaguez Incident, decision makers relied on NSA's timely and focused intelligence reports for critical information on the Khmer Rouge's reaction to the Marine rescue operation.

The BELLFIELD concept was further refined and was eventually incorporated into the design of the STU-I (Secure Telephone Unit) telephone system, but again the cost of the units was a major issue. The STU-I, in its final version, cost $35,000 each and still required supporting equipment equal to a two-drawer safe. Based on cost, the DoD limited the purchasing of the phones.

While the work on the STU-I validated the BELLFIELD concept, cost and other drawbacks would lead to its discontinuance. Nevertheless, the critical research done on these systems led to the development of the STU-III, a device that met both the cost and efficiency standards that had been so hard to achieve in the past. Eventually, the STU-III would become ubiquitous within the intelligence and defense communities and set the stage for even greater achievements in the realm of secure voice.

Remote Control Cryptology

As the '70s advanced, the need for versatile and creative approaches in technology increased. During this decade, NSA, for the first time, used the highly successful concept of remoting to enhance and improve its operations. This initiative was made possible by other advances in satellite collection, communications, and computing.

Collection of foreign signals from stationary facilities is expensive. By the mid-1960s, NSA leaders were growing increasingly concerned about the high cost of its foreign operations and started exploring options. In addition, many nations around the world were averse to allowing Agency assets within their borders.

Early successes helped NSA researchers to fully explore satellites for relaying communications around the globe. Concepts were developed in the early to mid-1960s for COMINT signals to be collected remotely. These signals could then be forwarded by satellite for processing. Several innovative approaches developed during the Vietnam War showed the potential of remoting operations and provided an incentive for accelerating the development of the technique. Finally, remoting was both efficient and increasingly cost effective, which allowed the Agency to reduce the number of sites and personnel overseas. Because it is both effective and efficient, remoting is still a vital part of Agency operations.

Catching Up and Staying Ahead

In the 1950s and into the 1960s, NSA and the Service Cryptologic Agencies (now known as "Components") led the country, if not the world, in computer development. By the 1970s, however, the computer industry outside NSA had changed from a few elite users to a market driven by heavy business use. Universities moved from offering a few computer-related courses to advanced degree programs in computer science. The outside world was catching up, and perhaps overtaking the cryptologic community in this field.

NSA wisely took advantage of the burgeoning outside expertise and wider availability of equipment. The sheer volume of signals acquired daily could be processed only with assistance from computer technology.

In the mid-1970s, NSA was moving toward desktop terminals, with offices making their own decisions about types of equipment and products. The terminals were not generally assigned to individuals during these early years, but rather were available as an office resource.

As more offices began relying on computers, disparate groups of users emerged, each favoring different, and often incompatible, systems. In 1974, building on an idea pioneered by the Defense Advanced Research Projects Agency, NSA established an interconnecting system known as PLATFORM, which centered computer operations on four core host complexes. The new system allowed for the use of a variety of interactive systems around the Agency. It would be some time before an Agency-wide initiative was implemented, bringing NSA fully into the Information Age.

In the 1960s, NSA worked with the Defense Intelligence Agency to develop COINS

(Community On-line Information System), that gave intelligence customers direct access to stored SIGINT data. This immediate access was revolutionary – customers could now get intelligence quickly. In 1972 another database, SOLIS (SIGINT On-line Information System), began storing actual SIGINT product, making it more widely available and permitting faster searches. Both systems pointed to a time when a comprehensive intelligence information sharing network would no longer be a dream, but a practical reality.

People

The cultural and demographic changes of the 1970s were reflected in different ways within the Agency workforce.

As the Vietnam War ended, NSA, along with the other members of the defense and intelligence communities, took big cuts in its budget and staffing levels. In addition to a smaller workforce, promotions were frozen. Compounding the problem, the average grade level of NSA employees was above that of other government agencies. This meant that over time personnel costs consumed an increasingly larger share of the Agency's budget.

The demographics of the workforce also posed challenges to management. VADM Inman concluded that the Agency had able leadership, as most senior people were still from the World War II generation. He believed that what he called the "Korean War generation" was well

VADM Inman and Ms. Ann Caracristi, who would go on to be the first woman to serve as Deputy Director, listen to Hall of Honor cryptologist Frank B. Rowlett describe the SIGABA machine.

prepared to take over, but what about the leaders coming after them?

With this challenge in mind, Inman created an executive career panel, giving it the task of identifying the "water walkers" in mid-level management. Once he received the list, Inman surprised everyone by demanding that all personnel on the list be assigned a different job within the next year. This began a practice of increased career diversification for those tapped for higher office. Inman was proud to find later that almost all the people on the list went on to senior positions, including two who became Deputy Directors.

Based largely on the success of Inman's initiative, NSA henceforth carefully orchestrated the selection and professional education of the Agency's future senior and mid-level managers.

Equal Opportunity Challenges

From its inception, minorities and women were under-represented in management at NSA. Making accommodations for disabilities was not yet common, but The Federal Rehabilitation Act of 1973, and subsequent legislation, gave agencies guidance on how to provide reasonable accommodations. Discrimination against individuals with an alternate lifestyle was still the rule at NSA. These constraints on Agency personnel were inconsistent with the changing civil rights/equal opportunity climate in the United States and deprived the Agency of potential talent.

Minorities

During World War II, the first African Americans in cryptology worked in segregated offices. Unfortunately, race policy at NSA was similar to other government organizations in the DC area. By the 1960s, however, the Agency's Office of the Inspector General (IG) launched a thorough investigation of personnel at all levels, into the wide disparities among categories of employees.

Based on the results of the investigation that clearly showed a pattern of discrimination, the IG made strong recommendations to the Director for the establishment of an Equal

Mrs. Minnie M. Kenny

Having grown up in Philadelphia, Pennsylvania, Minnie Kenny was amazed by the discrimination she found when she came to Washington for employment, and since joining NSA's predecessor in 1952, worked tirelessly throughout her career to further the cause of minorities in the Agency.

She quickly developed a reputation for excellence in several skill areas and was invited to work at an elite "think tank" at NSA, studying the future of cryptanalysis and language problems.

When the status of the Office of Equal Employment Opportunity (EEO) was in doubt, Mrs. Kenny convinced the NSA Director that the EEO should answer directly to him, thereby giving the EEO the status needed to be effective. Its successor organization, the Equal Employment Opportunity and Diversity (EEOD) Directorate still reports to the Director today.

Mrs. Minnie Kenny, through her superior job performance and commitment to the advancement of minorities in the Agency, became an inspiration to all. ■

Mrs. Minnie Kenny

Employment Opportunity (EEO) office and for a positive program to educate the workforce on EEO issues. The Director accepted both recommendations and initiated them in the late 1970s. Since then, hiring and recruitment practices have significantly improved minority representation in the workforce

Gender Challenges

Also during the 1970s, NSA found itself grappling with charges of gender discrimination.

Renetta Predmore had been noted as a promising employee, likely to advance in grade at NSA. However, she ran into the classic "glass ceiling." Predmore found credible evidence that she was the victim of gender discrimination in a promotion cycle, and she appealed the decision internally. When her appeal was rejected, she sued. On June 1, 1976, the United States District Court for the District of Maryland issued a decision in a landmark case that directly changed internal policies at NSA. The federal court decision in her favor changed the way promotions and eventually other important job decisions, such as field assignments, were handled.

This June 1976 decision directed that all boards or panels convened in the promotion process have a female member with an equal vote. Going forward, all promotion boards and career development and advancement boards were enhanced with minority and female representation.

Thanks to the changed climate for women that Ms. Predmore's suit brought about, those women already on board, as well as the new hires, were afforded opportunities that previously might have been denied them. The system changed for them, as one NSA senior manager put it, "because [Ms. Predmore] had the moxie, the guts to take on the Agency."

Sexual Orientation

In addition to race and gender issues, NSA also confronted prejudices related to sexual orientation. In the late 1970s, prompted by a potential court case, VADM Inman approved the hiring of a homosexual who openly revealed his sexual preference. Inman imposed some conditions designed to minimize the possibility of blackmail or other security risks feared by the Intelligence Community. The person, a linguist, had to "out" himself in person to his entire family and obey local laws on homosexuality. He also had to take an annual polygraph examination.

The prejudice at NSA about sexual orientation took longer to fall than those of gender and race, but significant progress on all three was made over the ensuing decades. NSA recognized that mission can be accomplished only through bringing together a diversity of views, skill sets, race, ethnicity, and gender to best serve the national security interests of our country. ■

National Security Agency
Historic Documents

Document A – Department of Defense Directive Implementing National Security Council Intelligence Directive 6

Document B – Transcript of Lt Gen Lew Allen's testimony before Congress

Document C – Front page of USSID guidelines

Document D – Memorandum describing U.S. response to dealing with "the Soviet microwave intercept problem"

DOCID: 3983926

Department of Defense

DIRECTIVE

NUMBER 5100.20

December 23, 1971

Incorporating Through Change 4, June 24, 1991

ASD(I)

SUBJECT: The National Security Agency and the Central Security Service

Reference: (a) National Security Council Intelligence Directive No. 6[1]

1. PURPOSE

This directive prescribes authorities, functions, and responsibilities of the National Security Agency (NSA) and the Central Security Service (CSS).

2. CONCEPT

2.1. Subject to the provisions of NSCID No. 6, and the National Security Act of 1947, as amended, and pursuant to the authorities vested in the Secretary of Defense, the National Security Agency is a separately organized agency within the Department of Defense under the direction, supervision, funding, maintenance and operation of the Secretary of Defense.

2.2. The National Security Agency is a unified organization structured to provide for the Signals Intelligence (SIGINT) mission of the United States and to insure secure communications systems for all departments and agencies of the U.S. Government.

2.3. The Central Security Service will conduct collection, processing and other SIGINT operations as assigned.

[1] Declassified on May 22, 1990 by the Director of Administration and Management, Office of the Secretary of Defense (Authority: E.O. 12356, April 6, 1982).

1

Document A: Department of Defense Directive that defined the authorities, functions, and responsibilities of the National Security Agency and Central Security Service in 1971.

DOCID: 3978970
Approved for Release by NSA on 06-14-2012 pursuant to E.O. 13526

29 OCTOBER 1975

I. STATEMENT OF LT GENERAL LEW ALLEN, JR., DIRECTOR NATIONAL SECURITY AGENCY

MR. CHAIRMAN, MEMBERS OF THE COMMITTEE

I RECOGNIZE THE IMPORTANT RESPONSIBILITY THIS COMMITTEE HAS TO INVESTIGATE THE INTELLIGENCE OPERATIONS OF THE UNITED STATES GOVERNMENT AND TO DETERMINE THE NEED FOR IMPROVEMENT BY LEGISLATIVE OR OTHER MEANS. FOR SEVERAL MONTHS, INVOLVING MANY THOUSANDS OF MANHOURS, THE NATIONAL SECURITY AGENCY HAS, I BELIEVE, CO-OPERATED WITH THIS COMMITTEE TO PROVIDE A THOROUGH INFORMATION BASE, INCLUDING DATA WHOSE CONTINUED SECRECY IS MOST IMPORTANT TO OUR NATION.

I AM NOW HERE TO DISCUSS IN OPEN SESSION CERTAIN ASPECTS OF AN IMPORTANT AND HITHERTO SECRET OPERATION OF THE U.S. GOVERNMENT. I RECOGNIZE THAT THE COMMITTEE IS DEEPLY CONCERNED THAT WE PROTECT SENSITIVE AND FRAGILE SOURCES OF INFORMATION. I APPRECIATE THE CARE WHICH THIS COMMITTEE AND STAFF HAVE EXERCISED TO PROTECT THE SENSITIVE DATA WE HAVE PROVIDED. I ALSO UNDERSTAND THAT THE COMMITTEE INTENDS TO RESTRICT THIS OPEN DISCUSSION TO CERTAIN SPECIFIED ACTIVITIES AND TO AVOID CURRENT FOREIGN INTELLIGENCE OPERATIONS. IT MAY NOT BE POSSIBLE TO DISCUSS ALL THESE ACTIVITIES COMPLETELY WITHOUT SOME RISK OF DAMAGE TO CONTINUING FOREIGN INTELLIGENCE CAPABILITIES. THEREFORE, I MAY REQUEST SOME ASPECTS

Document B: Congressional testimony transcript of NSA Director, Lt Gen Lew Allen, on NSA's 1967-1973 "Watch List" operation. (Full transcript on DVD)

DOCID: 3983925

~~TOP SECRET~~ 28 Jul 72 File Copy 173

National Security Agency

Fort George G. Meade, Maryland

29 SEPTEMBER 1971

Declassified and approved for release by NSA on 07-06-2012 pursuant to E.O. 13526

Superseded by USSID 1, 28 Jul 72

UNITED STATES SIGNAL INTELLIGENCE DIRECTIVE 1

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

Document C: Established in 1971, the USSID System provided timely procedural guidelines for practitioners throughout the SIGINT system.

MEMORANDUM

1989X
(Ref: 722X)

NATIONAL SECURITY COUNCIL

INFORMATION/ACTION
5 April 1976

~~TOP SECRET~~/XGDS-5B-(2)&(3)

DECLASSIFIED
E.O. 13526 (as amended) SEC 3.3
NSC 07-111, #8
NSC letter 7/15/11
By dal NARA, Date 9/13/11

PHOTOCOPY FROM GERALD FORD LIBRARY

MEMORANDUM FOR: BRENT SCOWCROFT

FROM: ROBERT SMITH

THROUGH: DAVID ELLIOTT

SUBJECT: Soviet Microwave Intercept Problem

You asked for items you could suggest to Secretary Rumsfeld to improve DOD's responsiveness in implementing the measures to deal with the Soviet microwave intercept problem. You also inquired as to the status of near-term steps, including movement to cable, increased monitoring, and jamming. These are summarized in the following:

I. Near-Term Measures

DUCKPINS I, the project to move all critical government circuits to cable in the Washington area, has moved and/or tagged approximately 9,000 circuits and is complete except for six AUTOVON satellite circuits which will be rolled off microwave within a few weeks. DUCKPINS II, which will extend similar protection to critical government circuits in the New York City and San Francisco areas, is now with the President for approval (copy at Tab A). These programs will secure all critical government circuits in all identified threat areas. DOD (DTACCS and DCA) has been very cooperative and responsive in these elements of the program.

We are limited in our monitoring of the Soviet take at the various intercept sites. More trained personnel and equipment could increase our coverage, and also allow us to undertake a survey of the other Bloc embassies to determine if they are carrying out interception. For technical reasons, however, we will be limited in our coverage at any individual site (e.g., at the Soviet Embassy, we might increase our coverage from about 2% to 10%).

~~TOP SECRET~~/XGDS-5B-(2)&(3)
Classified by: Brent Scowcroft

GERALD R. FORD

WARNING NOTICE — SENSITIVE
INTELLIGENCE SOURCES AND METHODS INVOLVED

Document D: National Security Council Memorandum to the National Security Advisor suggesting mitigating measures against the Soviet microwave collection of critical U.S. government communications.

A PERIOD OF GROWTH

1980s

In April 1981, Admiral Inman left NSA to become Deputy Director at CIA and was replaced by Lieutenant General Lincoln D. Faurer, USAF, NSA's tenth Director. An accomplished Air Force pilot, Faurer promoted revolutionary technological changes and developed a reputation as an innovator in the areas of secure communications and computer security. Faurer went on to serve in several important positions within the defense and intelligence communities, including Chief of the Defense Intelligence Agency's Space Systems Division, Director for Intelligence at U.S. Southern Command, and the USAF Deputy Assistant Chief of Staff for Intelligence.

In 1980 NSA appointed its first female Deputy Director, Ms. Ann Caracristi. Ms. Caracristi came to work as a cryptanalyst with the Army Signal Intelligence Service in 1942. Initially, she sorted Japanese Army messages, but quickly advanced to cryptanalysis and then management.

Her expertise and professionalism in responding to a wide range of tough and demanding cryptologic problems and challenges allowed her to advance quickly. In 1959 she was promoted to a supergrade, and in 1975 she became the first woman in the history of NSA to be promoted to GS-18. Caracristi's legacy and contributions not only inspired her female colleagues, but future generations of NSA employees of both genders.

A Shift in Focus

By 1980 it had become clear to U.S. policymakers that the USSR had no intention of giving up the battle to prevail over the United

President and Mrs. Reagan with LTG and Mrs. Odom at the dedication of new NSA buildings (OPS 2A/2B) - on September 26, 1986. (Video on DVD)

States and the West. Consequently, Soviet Russia and the Communist Bloc continued to be the major focus of the cryptologic community. It was also clear that other threats and challenges, particularly issues such as terrorism, would become part of the mix.

The Reagan administration made defense, foreign policy, and intelligence matters top priorities. To satisfy the administration's objectives, NSA received additional resources to shore up its mission capabilities. These resources assisted the Agency in its efforts to adapt to new and different threats and to maintain a high level of direct support to the military and civilian sectors of the government.

By the 1980s intelligence gathering on the Soviet target not only involved a large percentage of the cryptologic workforce, but also employed highly sophisticated intercept, processing, and analytic equipment, which relied heavily on sophisticated computing power.

During this time, NSA used fixed stations, airborne platforms, ground-based communications satellite dishes, geosynchronous and orbiting satellites and other assets to achieve its mission. It also worked in close coordination with the Service Cryptologic Elements in its efforts against the Soviet threat.

While much of the NSA effort against the Soviets remains classified, there are some unclassified examples of the Agency's cryptologic success during this time.

In 1983 the Soviet Union deliberately shot down KAL-007, a South Korean civilian airliner that had strayed into Soviet territory in the Far East (See Document A at end of chapter). The Reagan administration released to the public portions of voice intercepts that revealed that the Soviet MiG pilot involved knew that the aircraft was a civilian carrier. The tapes were able to show clearly that, despite this knowledge, the Soviets had ordered the pilot to shoot down the plane.

Courtesy Ronald Reagan Library

President Reagan and Soviet leader Mikhail Gorbachev signing a treaty reducing the size of their nations' nuclear arsenals, signaling the end of the Cold War.

NSA also provided intelligence support to the 1980 effort by U.S. policymakers to understand the background and reasons behind the political turmoil in Poland generated by the Solidarity movement. One of the more critical pieces of intelligence revealed that the Soviets would not invade Poland as they had Czechoslovakia in 1968. The success of the operation was due in part to the increased resources given to the Agency to track, observe, and gain an in-depth understanding of key intelligence targets.

In the midst of these successes, there were also constant reminders that both NSA and the Nation faced a worthy adversary. In the post-Cold War period the former Soviet Union is sometimes perceived as a lumbering giant on the path to obscurity. However, there were also times when the USSR demonstrated that it was still a formidable opponent. One of the most compelling examples of its prowess was uncovered through Project GUNMAN. Equally impressive perhaps, was the ability of the Agency to discover what the Soviets were up to.

Project GUNMAN: Much More Than a Typewriter

During the '80s NSA learned that the Soviets had planted a highly sophisticated "bug" in equipment, presumably in Moscow, used by a U.S. ally. This led U.S. and Agency leaders to investigate the possibility that the Soviets had been able to compromise U.S. equipment in the same way.

Project GUNMAN, as it was referred to, would be one of the most intense and secretive projects conducted by the U.S. Government at the time. America needed to know that the communications and activities of its foreign embassies around the world were secure. Any potential compromise to the integrity of U.S. operations abroad was simply unacceptable.

The Agency's first step in investigating the extent of the Soviets' success was to swap out every piece of electrical equipment in the U.S. Embassy in Moscow. Despite the obvious logistical and administrative challenges, any device that was plugged into a wall socket was removed and replaced.

LEADERSHIP

DIRECTORS

VADM Bobby Ray Inman, USN
(July 1977 – March 1981)

Lt Gen Lincoln Faurer, USAF
(April 1981 – May 1985)

LTG William E. Odom, USA
(May 1985 – July 1988)

VADM William Studeman, USN
(August 1988 – May 1992)

DEPUTY DIRECTORS

Anne Z. Caracristi
(April 1980 – July 1982)

Robert E. Rich
(July 1982 – July 1986)

Charles R. Lord
(July 1986 – March 1988)

Gerald R. Young
(March 1988 – July 1990)

"The Year of the Spy"

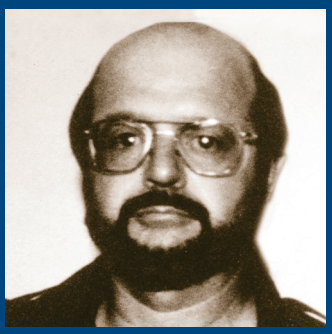
The Soviet Union would prove to be a worthy adversary, not only in the realm of technology, but also in exploiting the human frailties of well-placed individuals within the U.S. defense and intelligence communities, such as John Anthony Walker and Ronald William Pelton. Because of these two high profile incidents, 1985 would be dubbed by the media as the "Year of the Spy."

Pelton and Walker

In the mid-1980s, U.S. Intelligence Community leaders expressed growing concern over the fact that numerous sophisticated signals collection operations against the USSR had become increasingly less productive. Time would reveal the reason for their suspicions. Former NSA employee Ronald William Pelton had been providing classified information to the Soviets on a wide range of Agency sources and methods.

During his time at the Agency, Pelton had served as a mid-level analyst in "A Group," the NSA organization that targeted the Soviet Union. He had worked the Soviet problem for 20 years, both in uniform and as a civilian and was a specialist in collection technology. He had also written an operational manual for at least one major collection project. Worst of all for NSA, he possessed a photographic memory. Due to financial concerns, he resigned from the Agency in the 1970s. After resigning, his financial situation would go from bad to worse.

Ronald William Pelton



John Walker

Looking for a way to solve his financial troubles, in 1980 he visited the Soviet Embassy in Washington and offered his assistance. Over the next few years the KGB questioned him extensively. Despite his hopes for a big payday from his Soviet handlers, Pelton would be paid poorly by the KGB for the information he provided. However, the secrets he would betray would end up costing the U.S. millions of dollars and do grave damage to U.S. intelligence operations.

Pelton was caught in 1985 when a KGB defector informed his U.S. handler that a "walk-in" contact at the Soviet Embassy in Washington had been a former NSA employee. This led to an FBI investigation that eventually identified him as the spy in question. He was arrested on November 25, 1985.

Rather than seek a plea bargain, the Justice Department, with NSA and CIA concurrence, took him to trial. During the proceedings great care was taken to protect Agency sources and methods. The jury found Pelton guilty, and he was sentenced to three consecutive life terms plus ten years for his crimes against the Nation. In 1992 Pelton wrote the Agency a letter of apology, saying "My actions were un-forgivable [sic]."

Soviet espionage activities also affected the COMSEC side of Agency operations. During the 1980s, it was discovered that since 1967 U.S. Navy Petty Officer John Walker, abetted by family members and a friend, had been stealing and selling the punch cards that controlled U.S. cryptographic devices. This compromise enabled the Soviets to read U.S. Navy encrypted messages. John Anthony Walker was given a life sentence for his crime.

The discovery of Petty Officer Walker's treachery led to widespread adoption of Over-the-Air-Rekeying (OTAR) of cryptographic equipment. The Walker and Pelton espionage cases of the 1980s demonstrated the need for this new capability in peacetime, as well as wartime. ■

The next phase of the project was an intense technical analysis of the collected items. Over the next few weeks a corps of experts from the COMSEC organization carefully examined each electrical device in exacting detail. Finally in late July, a technician, using x-ray photos of components taken from an IBM Selectric typewriter, discovered a small device capable of recording, storing, and transmitting the keystrokes of the typewriter. Next the other entities were checked for similar kinds of devices. In the end a total of 16 similar "bugs" turned up in typewriters from the Moscow Embassy and the U.S. Consulate in Leningrad.

The third step in the operation was perhaps the most difficult. Knowing that the devices had been in place for at least five years, NSA analysts were now duty bound to evaluate the extent and duration of the compromise.

News of the operation eventually leaked out to the press and became public knowledge, reminding the Nation that the Soviet Security Services were still highly capable foes.

Due to the Agency's success in GUNMAN, other components of the U.S. Government began to look to the Agency for technical expertise and advice on a wide range of security challenges. The Agency assumed new responsibilities in keeping the electronic communications of U.S. establishments overseas secure and safe. These responsibilities added a new and vital dimension to the Agency's collective technical knowledge and abilities that would better serve the Nation in years to come.

A Worldwide Enterprise

While most Agency assets were still devoted to the Soviet threat, other areas and regions around the world began to consume more of the Agency's attention in the 1980s.

In 1987 intelligence derived from Agency operations confirmed that Iraqi dictator Saddam Hussein had used poison gas against the Kurdish population of his own country.

Also during that year, largely in response to rising tensions with Iran, President Reagan authorized the U.S. Navy to escort Kuwaiti tankers sailing through the Persian Gulf. During this potentially dangerous situation, NSA provided critical cryptologic support to the U.S. Navy elements involved in the operation.

By participating in these events, the Agency gained valuable experience in providing communications technology in direct support of deployed U.S. military forces. The lessons learned from these operations would pay off a few years later when NSA was called on to support U.S. and allied military forces during Operation Desert Storm.

In addition to its activities against selected nation states, the Agency was also dealing with a growing list of transnational threats and targets.

One of the most challenging of these emerging threats was the flow of narcotics into the United States. Over time, NSA and its partners in the Intelligence Community became an integral part of the effort to stop the entry of narcotics into the country.

Initially, NSA's contribution to counternarcotics had been limited, particularly after laws more strictly defining foreign intelligence were passed after congressional hearings in the 1970s. However, as the flow of narcotics into the United States posed a greater threat to the national security, the Agency worked with the appropriate authorities and institutions to develop new collection guidelines.

Counternarcotics were not the only non-traditional area that the Agency became involved with during the decade. The rise of worldwide terrorism in the 1970s required strong Agency support to U.S. military leadership which was key in resolving several highjacking incidents. From these incidents, the Agency would gain valuable insight into the workings of terrorist communications and networks. Unfortunately, these new skills would be put to use many times in the future.

President Reagan Visits NSA

Since its inception in 1952 NSA had been visited by Vice Presidents Humphrey and Rockefeller, but never by the Commander-in-Chief. In September 1986, however, the Agency would host its first presidential visit when President Ronald Reagan agreed to come to Ft. Meade to dedicate two new buildings on the NSA campus.

The new structures, known as Operations 2A and 2B, were shielded in copper to prevent unintended emanations from electronic equipment. With the addition of these two structures, the main NSA complex on Fort Meade became known as "the Big Four." OPS 2B would replace the Headquarters Building as the home of the Director (Video clip of dedication ceremony available on DVD).

Lieutenant General Odom

In May 1985, Army Lieutenant General William E. Odom, was tapped by the administration to replace General Faurer. Odom was an intellectual who had earned a master's degree in Russian area studies and eventually a Ph.D. in political science. He also had a close relationship with several administration leaders, including former President Carter's National Security Adviser, Zbigniew Brzezinski. Previously Odom had served as an Assistant Army Attaché in Moscow and as a West Point professor. Prior to coming to NSA, he had been Assistant Chief of Staff for Intelligence, U.S. Army. One of General Odom's priorities was to enhance the Agency's ability to meet the needs of national intelligence policymakers.

Backing the Attack

Throughout the 1980s, NSA stressed the need to improve timely and agile support to the military. To achieve this goal, General Faurer ensured that NSA was included in planning for future military operations.

In the mid-1980s, the Department of Defense (DoD) worked with Congress to pass the Goldwater-Nichols Department of Defense Reorganization Act of 1986 to realign functions within DoD to achieve greater efficacy. The Act designated NSA as a Combat Support Agency. This designation clearly identified the NSA's capacity to support military operations and set in motion a series of initiatives that would allow the Agency to fulfill its newly defined role.

By 1989, when President George H. W. Bush ordered an invasion of Panama to oust its dictator Manual Noriega, NSA had become a vital part of global military operations everywhere and assisted with the planning and execution of this successful operation.

The term combat support generally denotes efforts by organizations like NSA to develop information on enemy plans and operations prior to their execution. However, for a cryptologic organization, combat support also involves protecting information on the battlefield.

From a cryptologic perspective, the Vietnam War served as a laboratory for testing new technology in combat. NSA's leadership, in conjunction with the Service Cryptologic Agencies, recognized that the lessons learned in the jungles of Southeast Asia could improve future cryptologic support operations. The demands of the climate and terrain of a proposed area of operation prompted the cryptologic community to find innovative ways to support troops in the field. Increased computerization would prove to be a significant part of the solution to these challenges.

Included in this support was the new found ability to use national assets – such as massive banks of computers – for tactical support to deployed forces. This capability became an important factor as the cryptologic community mobilized to support U.S. and coalition forces in Operation Desert Storm at the beginning of the next decade.

A Computer on Every Desk

But protecting information on the battlefield was only one of many challenges of the time. On the home front, the Agency was seeking to find ways to harness computer technology to serve its growing needs. NSA began to work toward the goal of putting a computer on every analyst's desk and investing in and developing supercomputer technology.

As had been the case in the past, the research element of this effort was crucial in developing specific key supercomputer applications. Recognizing this, the research directorate pressed their requirement for a dedicated research facility and was eventually able, with the support of General Faurer, to build a state-of-the art Supercomputer Research Center.

STU (III)-PENDOUS

Although the 1970s-era STU-II (Secure Telephone Unit – second generation) had proved its worth, COMSEC leaders saw room for improvement and sought to create the next generation of secure communications devices to provide even higher levels of security and performance.

The result was the STU-III (Secure Telephone Unit - third generation). The STU-III was developed through a combined effort of Agency and private industry partners well versed in communications technology. The new device was a huge improvement over previous models, primarily because it could be produced at a relatively low cost.

Most importantly, the STU-III provided vastly improved security, better voice quality, and faster data transfer capability. The device was the first large-scale implementation of public key cryptography and Over-the-Air-Rekeying, a concept that had been developed during the Vietnam War. (See Document B at end of chapter.)

The STU-III program proved to be one of the greatest success stories in the history of NSA. Eventually, more than 350,000 units were fielded and remained in service well into the twenty-first century.

Looking Overhead

In previous decades NSA and CIA disagreed over SIGINT authorities and practices. In the 1980s NSA confronted similar issues with the National Reconnaissance Office (NRO), the agency tasked with managing the Nation's satellite programs. While the NRO controlled technical aspects of the collection of foreign signals by satellite, NSA often was responsible for processing and disseminating the intelligence information

The NSA Police Force

After the departure of the U.S. Marine guards in 1978, security functions at NSA were transferred to the Federal Protective Service, a division of the General Services Administration (GSA). In October 1986 GSA returned the authority for security measures to the NSA Director, which facilitated the establishment of a police force, fully controlled and operated by the Agency.

The Agency's newly established Security Protective Force eventually assumed all the functions of the previous units, including protection of NSA assets and emergency services. The Agency's commitment to ensure that all members of the force were properly trained enabled them, when needed, to serve alongside neighboring state and municipal forces. By the end of the century, NSA had one of the largest police forces in Maryland. Today the NSA Police continue to protect NSA affiliates and buildings throughout NSA's worldwide enterprise. ■

Since 1986, NSA's formally trained police force, using state-of-the-art technology, has controlled entrance into NSA facilities.

culled from the operations. Due to the unsettled division of labor, NSA's leadership was not entirely comfortable with some NRO approaches, and the relationship became strained to the point where action needed to be taken to ensure the effectiveness of the program.

In 1984 NSA and NRO hammered out an agreement that established a new organization, the Overhead Collection Management Center (OCMC). The OCMC, modeled on Defense Special Missile and Aerospace Center, was to be centered at NSA headquarters with an NSA affiliate as Director. The deputy of the entity would be from the NRO with the CIA having authority over and appointing the chief of requirements. In the end, the solution pleased all of the parties involved and, most importantly, promoted effective operations. This collaboration foreshadowed the current extensive integration of the Intelligence Community.

Vice Admiral Studeman

As the decade came to a close, the Agency welcomed its third Navy Director, Vice Admiral William O. Studeman. Studeman began his career as a Navy Air Intelligence Officer and later served in assignments for the Seventh Fleet and DIA. His hard work and experience in the intelligence arena culminated in his being named Director of Naval Intelligence. Studeman would exert strong leadership through the challenging and unexpected collapse of the USSR and successfully see the Agency through the Desert Storm campaign.

Admiral Studeman left NSA in 1992 to become Deputy Director of the CIA, where he later also served as acting Director. ■

President George H.W. Bush confers in confidence using a STU III device.

National Security Agency
Historic Documents

Document A – Presidential statement on the Korean flight KAL 007 shoot down

Document B – Memorandum from NSA to Deputy Under Secretary of Defense on DoD proposal for public cyptography

Washington, D.C. 20520

3

STATEMENT

As part of the policy of the US Government to develop full information on the tragic shootdown of KAL 007 by Soviet forces on August 31, U.S. Government experts have continued to review the poor quality transmission on the tape which was played at the UN Security Council September 6. That review has now been completed. After efforts at electronic enhancement and hundreds of replays of the tape, U.S. Government linguists were able to interpret three passages more clearly as indicated below.

The first segment at 1819:08 which originally was translated "I have enough time," now is translated as "they do not see me." The second segment was a previously unintelligible phrase at 1820:49, which has now been translated as "I am firing cannon bursts." Because of the Soviet pilot's reference at 1828:05 to launching "both" rockets, the linguists also rechecked the reference at 1823:37 which was previously translated as "rocket." They were able to clarify that the plural was used; thus the translations should be "..., now I will try rockets."

The transcript does not indicate whether the cannon shots were aimed at the KAL plane or were tracer rounds. We do note that, according to information made available by the Government of Japan to the United Nations, KAL 007, in its routine radio transmission to Tokyo at 1823* (over two minutes after the cannons were fired) gave no

* "18:23 GMT (3:23 JST)
KE-007: Tokyo Radio Korean Air 007 level 350 (Altitude 35,000 feet).
RJAA: Korean Air 007 Tokyo Roger."
--from the September 7, 1983 statement by the Director-General of the Public Information and Cultural Affairs Bureau of the Ministry of Foreign Affairs of Japan.

Document A – Presidential statement from Ronald Reagan reinforcing the U.S. and Japanese position on the details and conclusion of the Korean flight KAL 007 shot down by the Soviet government.

DOCID: 3978871

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755

P.L. 86-36

Serial: N1053
7 October 1980

Approved for Release by NSA on 06-14-2012 pursuant to E.O. 13526

MEMORANDUM FOR THE DEPUTY UNDER SECRETARY OF DEFENSE (POLICY REVIEW

SUBJECT: National Policy on Public Cryptography

1. Please refer to your DUSD (PR) memorandum I-08944/80, 22 September 1980, subject "National Policy on Public Cryptography."

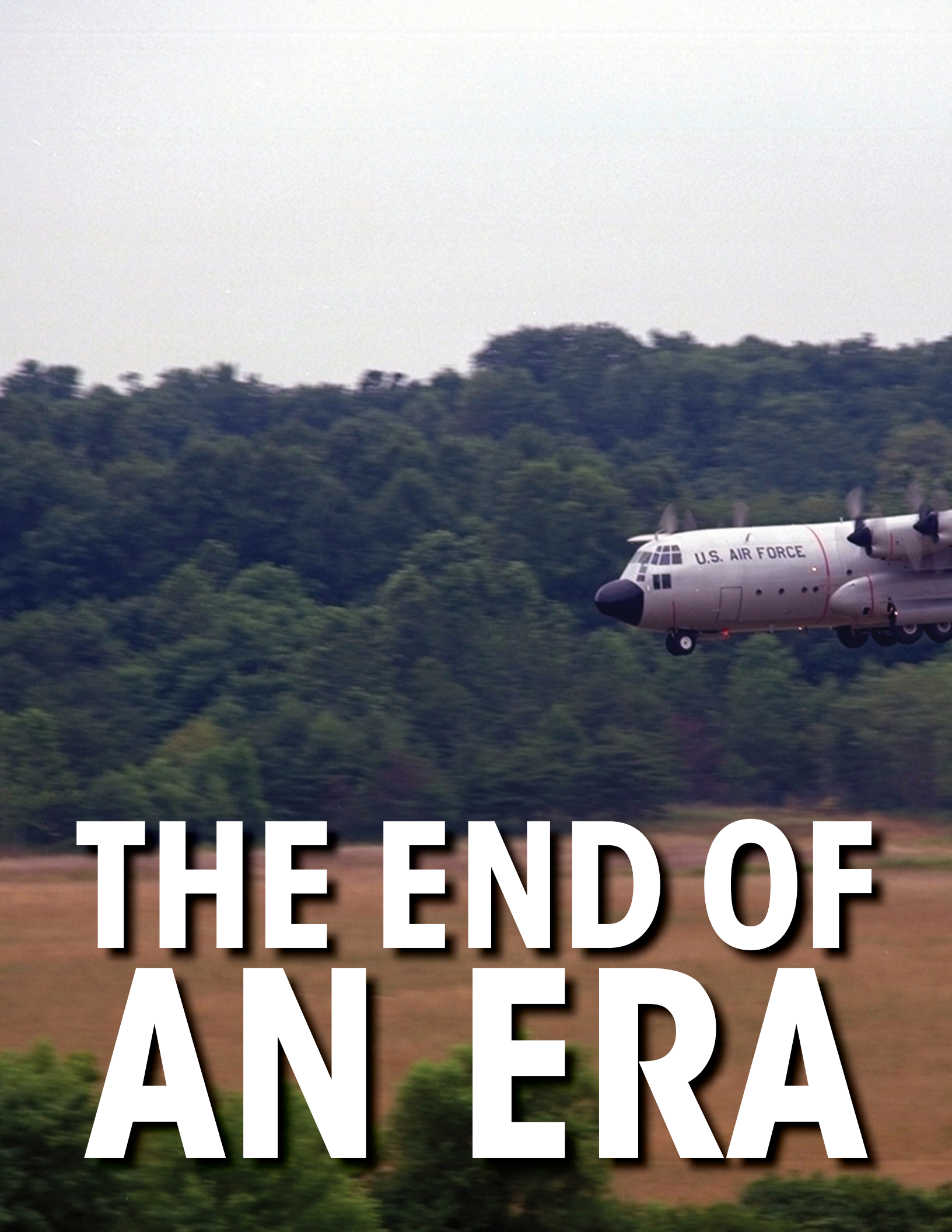
2. While progress has been achieved in identifying the principle issues involved in a national policy on public cryptography, I have serious reservations concerning the proposed DoD response to Dr. Press and cannot support it in its present form. It would be most counter-productive to forward this response to Dr. Press without major modification as to both specific content and general philosophy.

3. I believe that the response does not describe the significant differences of opinion that have evolved between Defense and Commerce regarding many of the identified issues. We have not agreed with the proposed policy positions on Issues No. 1 and 2 and have earlier provided alternative statements for these issues. Despite our earlier submissions to you, as currently drafted the proposed positions do not protect the Government's legitimate national security concerns nor accommodate the results of NSA's recent work with the American Council on Education's (ACE) Study Group on Public Cryptography.

4. The issues analysis in the draft Appendix A does not represent, as implied in the introductory paragraph of the Summary, any sort of agreement between DoD and DOC participants and, as such, is misleading. Because of the lack of consensus concerning the "YES" and "NO" points included in each issue analysis, the points are confusing and misleading. I recommend that the "YES" and "NO" points be deleted and that only a list of the Issue statements and their respective DoD policy statement positions be forwarded to Dr. Press. In addition, I suggest that the penultimate sentence of the Summary be revised to read "Each policy statement represents only the Department of Defense position; it should be understood that the issues analysis undertaken jointly with the Department of Commerce surfaced broad disagreement regarding the factors impacting on each issue as well as the policy positions themselves." With this change, the final sentence of the Summary may be deleted.

5. I also recommend that the introductory paragraph to Section I be revised as follows:

Document B – Memorandum from NSA Director, Vice Admiral Bobby Inman, to the Deputy Under Secretary of Defense presenting his concerns about the DoD proposal for public cryptography.



THE END OF AN ERA

1990s

NSA and the CSS continued collecting signals from the Soviet Union and Warsaw Pact nations throughout the 1990s, right up until the fall of the Berlin Wall and the disintegration of the Soviet Union. NSA analysts, drawing on vast experience, provided unique intelligence information of significant value to national decision-makers and policymakers in peace, crisis, and war.

While there was rejoicing over the fact that United States and the West had "won" the Cold War, the end of the Soviet threat forced NSA and the Nation to adjust to a strange new world where few, if any, rules existed, and where asymmetrical warfare was now the rule rather than the exception.

The monolithic Soviet target was quickly replaced by newer targets, including non-state actors who made good use of the latest technology. Widely available commercial products enabled rapid and radical changes in communications methods and procedures, and targets displayed a growing knowledge of communications security techniques.

Lifting the Cryptologic Curtain

After the Cold War, NSA leadership began to consider ways that the Agency could be a bit more open in its relationship with the general public. From NSA's inception, security and anonymity had been the main watchwords and, since 1952, the curtain over the Agency had been pulled fully to the ground. Now, however,

The C-130 aircraft, pictured here landing at Fort Meade, was refurbished to resemble the C-130 downed by Soviets in 1958 and is the centerpiece of National Vigilance Park.

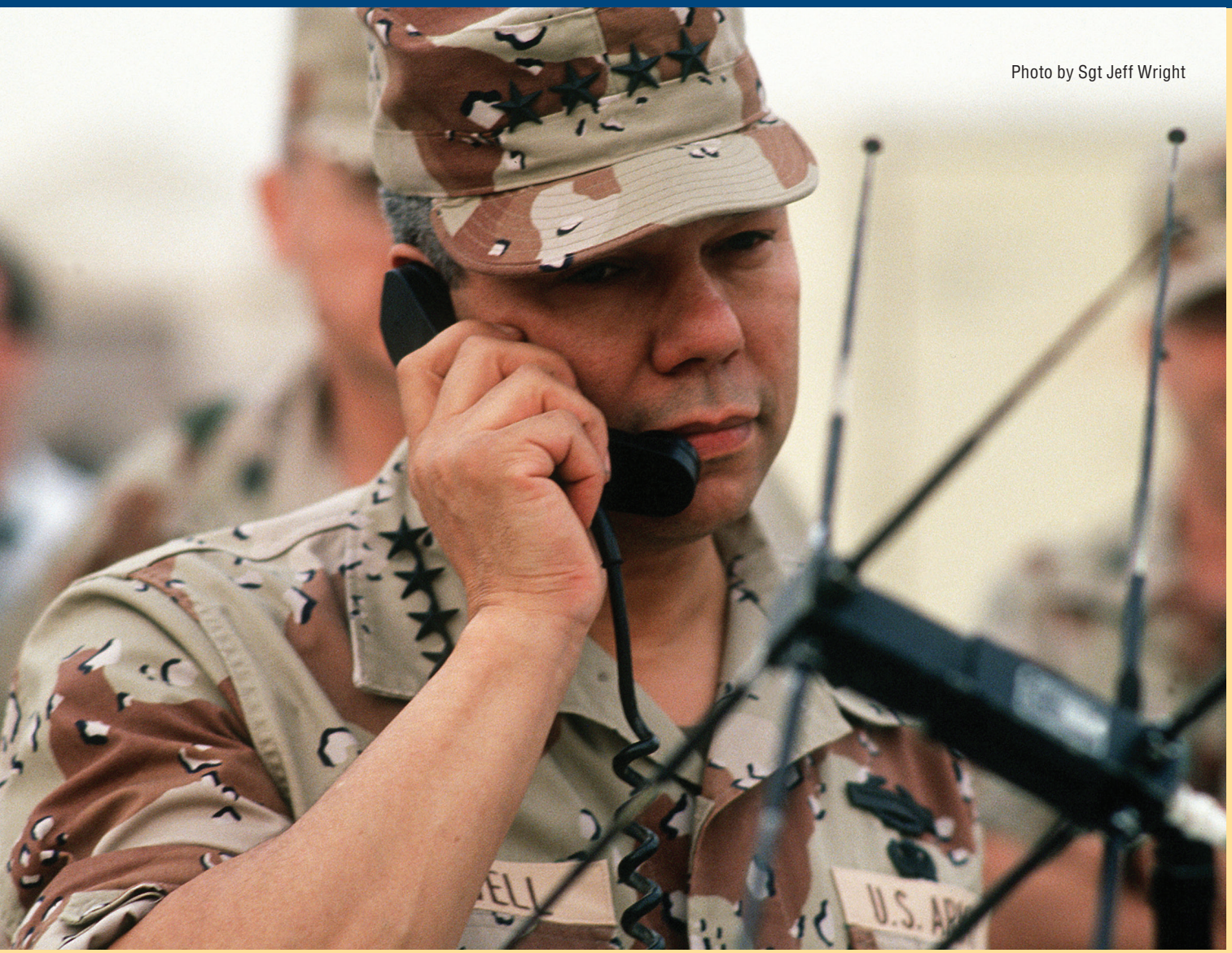


Photo by Sgt Jeff Wright

Chairman of the Joint Chiefs of Staff General Colin Powell uses NSA technology to communicate securely with the Pentagon during Operation Desert Shield.

Agency leaders began to ponder the prospect of raising it just a bit.

The move to openness would not be easy. The challenge was to engage the public enough to demonstrate the critical role NSA plays in defending the Nation while protecting sensitive sources and methods. Despite earlier efforts, large portions of the American public remained suspicious of the Intelligence Community overall and of NSA in particular.

Under Admiral Studeman, NSA, for the first time, publicly stressed the contributions of the organization to the economy of the Central Maryland region and the state in general. In addition, NSA began a series of locally based math outreach programs to promote the study of cryptology to faculty and students at local schools.

The National Cryptologic Museum

In the early 1990s Admiral Studeman took NSA's public outreach programs to a new level with the opening of the National Cryptologic Museum. Located on the edge of the main NSA campus, the new museum, with free admission and open access, quickly became a valuable tool to educate the public about the history and success of NSA. The museum also served as a means for helping the greater world to understand the indelible role that cryptology had played throughout human history.

In 1996, at the urging of Director Lt Gen Minihan, NSA created the National Vigilance Park (NVP). NVP was designed to honor those "silent warriors" who risked their lives performing airborne signals intelligence missions during the Cold War. The centerpiece of the park is a C-130 aircraft, refurbished to resemble the reconnaissance-configured C-130-A downed by Soviet fighters over Soviet Armenia in 1958.

The park also has on exhibit an Army RU-8D Seminole that honors those involved in airborne cryptologic intelligence-gathering missions during the Vietnam conflict, and a U.S. Navy EA-3B aircraft to honor the seven U.S. Navy crewmen who lost their lives in a similar aircraft during an operational mission in the Mediterranean in 1987.

Desert Storm

Having led the Agency through the aftermath of the collapse of the Soviet Union, Admiral Studeman remained at the helm during the Nation's first post-Cold War military operation – Operation DESERT STORM, the effort to free Kuwait from Iraq. NSA provided key SIGINT support during both DESERT SHIELD, the buildup phase, and DESERT STORM, the combat phase. Throughout the conflict, the Agency supplied the United States and the coalition with the information they needed to prevail, while providing secure tactical communications on the battlefield.

An Appreciative Leadership

In recognition of NSA's work during the conflict, President George H.W. Bush came to NSA to praise its employees for their support to DESERT STORM.

President Bush commended NSA employees as "the unsung heroes of DESERT STORM." He said, "Our success in the Gulf could quite literally never have happened without the dedication that's on display right here through all the days and all the nights of DESERT STORM."

General Colin Powell, Chairman of the Joint Chiefs of Staff, during DESERT STORM also visited NSA in 1991. He told the workforce that "no operational commanders, probably in the history of warfare, certainly in the history of

LEADERSHIP

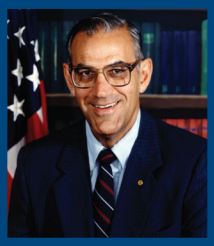
DIRECTORS

VADM William Studeman, USN
(August 1988 – May 1992)

VADM Michael McConnell, USN
(May 1992 – February 1996)

Lt Gen Kenneth A. Minihan, USAF
(February 1996 – March 1999)

Lt Gen Michael V. Hayden, USAF
(March 1999 – April 2005)



DEPUTY DIRECTORS

Robert L. Prestel
(July 1990 – January 1994)

William P. Crowell
(February 1994 – October 1997)

Barbra A. McNamara
(October 1997 – June 2000)

President George H.W. Bush describes NSA employees as "the unsung heroes of DESERT STORM."

American warfare, have had better insight into the strengths and vulnerabilities of the enemy."

Vice Admiral McConnell

In May 1992, Admiral Studeman was succeeded as Director NSA/Chief CSS by Vice Admiral J. Michael McConnell, USN. (See Document A at end of chapter.) A veteran of the Vietnam War, McConnell had spent most of his career in intelligence, rising through the ranks with assignments with the Director of Naval Intelligence; NSA (as Chief of the Naval Forces Division); DIA; and the Joint Chiefs of Staff. Upon assuming the position of Director, he was immediately confronted with the challenge of post-Cold War congressional mandates calling for downsizing in the intelligence and defense communities.

The Peace Dividend

As the Communist Bloc crumbled, America and its leaders began to call for a "peace dividend." For decades, the American people had been willing to "pay any price and bear any burden" to defeat the Soviet threat. Now the Cold War was over. The Nation debated what could be done with funds previously invested in robust defense and intelligence budgets. Congress responded to the public's call for cuts by mandating significant reductions in NSA's personnel and budget.

In response, Admiral McConnell tried to mitigate the effects of downsizing by working to preserve NSA's operational capabilities. At the same time he sought to save money by cutting the budgets of support elements, by reducing and consolidating overseas sites and personnel.

"They Served in Silence"

At a junction of heavily traveled hallways in the main NSA Fort Meade Campus stands a black granite wall flanked by flags. The NSA/CSS Cryptologic Memorial Wall is intended to honor and remember those who have give their lives, "serving in silence," in the line of duty since World War II.

The monument is a powerful symbol of six decades of Cryptologic endeavor and the determination of the NSA/CSS workforce to continue in dedicated service to securing the Nation's future.

The Memorial Wall, dedicated in 1996, was a project driven by VADM Michael McConnell. The striking monument, designed by an NSA employee, is a black granite rectangle, centered with a triangle. The three points on the triangle represent the cryptologists and their ideals that form the foundation of cryptologic work: dedication to mission, dedication to workmate, and dedication to country.

When the wall was originally installed, it listed 146 names. Sadly, in the intervening years, other cryptologists have also given their lives to protect the country's safety and liberty. At NSA's 60th anniversary, the Memorial Wall honors the memories of 170 fellow cryptologists.

Today's workforce recognizes and honors the ultimate sacrifice of those whose names are engraved on the Cryptologic Memorial Wall. ■

President Bill Clinton thanks Admiral McConnell for NSA support.

NSA and the Information Revolution

The 1990s saw the beginnings of the Information Revolution. Advancement in communications technology was happening rapidly, and it became increasingly difficult to keep pace with the changes. Simultaneously many in Congress and the Executive Branch began to view NSA as a lumbering agency that had lost its technical edge. For the first time, NSA and its partners in the defense and intelligence communities were forced to justify their existence to Congress and the Nation.

NSA was struggling to adapt to the technological challenges of the new geopolitical climate, as well as the tough realities of reorienting and retooling its workforce. Despite these challenges, Agency leaders were well aware of their responsibility to somehow find a way to maintain NSA's mission to provide and protect America's most important communications in an ever changing world.

Clipper Chip

Technology advances in the 90s forced the Agency to take new and different approaches to the challenge of securing communications. As more military and other government users required strong cryptography to protect communication devices or computers, it became apparent that traditional methods of producing cryptographic materials were no longer adequate. NSA increasingly turned to certification of commercial network security products for government use.

Admiral McConnell confronted the question of public cryptography while dealing with the downsizing of NSA. While the U.S. (and NSA) wanted to foster good protection for "friendly" entities in networked computers and cellular telephones, they were also concerned with keeping strong cryptography out of the wrong hands. The proposed solution was "the Clipper Chip," an arrangement by which the key to publicly available cryptography would be kept in escrow, but would be available to the federal government via a court-issued warrant when there were legitimate reasons for access.

The technology developed under Admiral McConnell's leadership was workable, but the Clipper Chip itself was deemed politically unacceptable. Fearful of potential misuses, the public and their government representatives solidly rejected the idea. Nevertheless, the encryption technology created for the Clipper Chip found other applications and was adopted for certain uses within the government.

Lieutenant General Minihan

In 1996, Admiral McConnell retired, leaving NSA in the hands of Lieutenant General Kenneth A. Minihan, USAF. Minihan had a long history of service in the Intelligence Community, including prior service as a mid-level supervisor at NSA, command of a field site, and of the Air Force's cryptologic component. Just prior to assuming the directorship at NSA, Minihan held the post of Director at the Defense Intelligence Agency, a key NSA partner.

General Minihan assumed command during a time in NSA's history when the Agency was struggling not only with its missions, but also with its identity. The end of the Cold War left NSA's future as an institution unclear. Budgets were shrinking, and

rumors were rife that NSA's key components might become separate organizations.

One Team One Mission

Citing the risk to networked information systems, Minihan maintained that the best response to the problems confronting NSA was to consistently combine and coordinate as much as possible on both sides of the cryptologic equation in carrying out Agency missions and objectives.

Minihan believed that by leveraging both missions at once, NSA could be more effective. He expressed the concept by coining the phrase "ONE TEAM, ONE MISSION" and urged the United States and its allies to work toward the goal of "information dominance on the world scene."

His efforts prompted the workforce to work more closely together and to look to the future. With the Agency's two missions working in tandem, the stage was set for NSA to have a blended mission in the next decade with the emerging cyber challenge.

By the mid-1990s CSS had become a true unified system with its own unique seal and identity and has proven to be a vital contributor to the U.S. intelligence and defense communities.

Today both organizations are fully integrated and continue to work together to protect the Nation.

Future Day

As part of his program for encouraging NSA personnel to turn their thoughts and energy toward the challenges ahead, General Minihan proclaimed October 17, 1996, as "Future Day." This day involved:

- A complete worldwide stand-down of all but the most essential activities.
- Traditional face-to-face discussion groups convened by topic to talk about Agency goals and how to meet new challenges.
- Agency-wide chat rooms, used probably for the first time, with General Minihan participating and connecting with the workforce electronically.

Lieutenant General Minihan

Although workforce participants differed in their evaluation of Future Day, dedicating a day to discuss the future forced almost everyone at NSA to recognize the inevitability of change and to consider the directions it might take.

Public Outreach

Under General Minihan, NSA for the first time opened its doors for the filming of a documentary about the Agency. Minihan and other Agency leaders recognized that misunderstandings about the role and intent of NSA's activities had to be addressed in order to secure the American people's trust and confidence.

Extending the Enterprise

In the 1970s and 1980s, NSA leadership grew concerned over the centralization of functions at Fort Meade. Partially prompted by the need to find adequate space for its personnel and equipment, the Agency began to look at moving some assets away from the Fort Meade area.

In this light, in 1980 a Remote Operating Facility (ROF) at Kunia was established on the Hawaiian island of Oahu. Although living costs were high

The aircraft on display at the National Vigilance Park honor the "silent warriors" who died performing airborne signals intelligence missions during the Cold War.

there, Kunia had the advantage of proximity to the Commander in Chief, Pacific (CINCPAC).

In the late 1980s, the cryptologic leadership began developing the Regional Security Operations Center (RSOC) concept. Proven computer and communications technology allowed NSA to delegate SIGINT authority to these regional centers, thus avoiding an overconcentration in the Washington area.

Under the RSOC doctrine, each center would be "hosted" by one of the military services so that all services could be represented.

In 1995 the centers opened and NSA began to transfer missions to them. The Kunia facility was given a new status as an RSOC.

Over the next decade, the RSOCs evolved from limited operations centers into mini "regional NSAs" in Georgia, Texas, Hawaii and Colorado with the following mission benefits:

- Consolidation of cryptologic operations
- Dispersion of facilities from the Washington, D.C. area
- Capability of serving as alternate communications centers
- Representation of all military services.

The concept of "regional NSAs" was reinforced when NSA suffered a massive computer outage early in 2000, and the RSOCs, as components that could operate independently, picked up the essential missions until NSA was back in full operation. Today all four centers, now known as Cryptologic Centers, are operational, expanding, and provide redundancy in the event of an emergency.

Expeditionary SIGINT

While resources were decreasing during the 1990s, customer requirements for NSA's services and products were not. To better serve the Agency's increasingly diverse customer set, NSA began deploying personnel as NSA/CSS representatives (NCR) or as part of Cryptologic Services Groups (CSG) to intelligence community partners and military commands. Their mission was to act as an advocate for the customer, assisting them in navigating the NSA enterprise and helping to interpret their requirements to NSA, in order to better respond to them. NCRs and CSGs were also charged with helping partners understand what the cryptologic system could, and could not, do for them.

In the years after Operation Desert Storm, NSA and its military partners in the CSS began considering how best to extend this type of close support to warfighters engaged in future operations. Changes in the nature of telecommunications and the capabilities needed to turn modern communications into actionable intelligence for military consumers led to an increasingly close partnership between the civilian and military components of the enterprise. Modern military commanders were as interested in the strategic "big picture" issues as they remained in the tactical environment on the battlefield.

The increasing military activity of the late 90s led to the birth of Expeditionary SIGINT.

While NSA continued to support military customers from Fort Meade and field sites around the world, the Agency also began pushing the resources of the enterprise closer to the warfighter. NSA personnel began joining their CSS colleagues in deployments with military forces, providing tailored SIGINT support to operations around the world.

Like the Cryptologic Centers, the NCRs, CSGs, and Expeditionary SIGINT personnel ensured continuity of operations for NSA's customers and increased NSA's ability to provide tailored support in response to critical requirements.

Enhanced Security

The 1990s also saw an increase in the level of physical security at NSA. Access became more restricted; no longer could family members and pizza delivery people get close to the fence line. After the Oklahoma City bombing in 1995, an NSA perimeter security fence was constructed to surround the entire Fort Meade campus. In addition, the NSA Police added a K-9 unit in 1998, which greatly improved the Agency's capability to check for explosives during commercial vehicle inspections and assist in security patrols and emergency responses.

Improving Computer Security

In the late 1990s, the NSA Systems and Network Attack Center (SNAC) tackled the difficult question of how best to improve the security level of personal computers and servers that were part of national security systems. This led to the need to discover software implementation flaws, probe operational networks for weaknesses, and develop guidance to harden systems against attack.

The SNAC made security configuration guidance publicly available on NSA's web page, and released guidance for the Department of Defense's (DoD) Windows operating systems and Unix-like operating systems.

Microsoft provided additional guidance with SNAC's full cooperation and public recommendation. The settings from this effort were adopted as a baseline for the DoD and by the National Institute of Standards and Technology for its Federal Desktop Core Configuration. Through this effort the federal

Regional Security Operations Centers, like the one in Hawaii pictured above, provide NSA with the redundancy needed in the event of an emergency.

government produced a common body of information describing a security baseline.

Over time, NSA's role in communications security expanded beyond the traditional goals of ensuring privacy among communicators. Officials realized that modern modes of communication required concern over protecting availability, integrity, authentication, confidentiality, and nonrepudiation.

This expanded notion led to yet another name change - from the Communications Security Organization to the Information Assurance Directorate (IAD), encompassing the full breadth of the mission set aimed at keeping our national security information systems secure.

In early 1999 General Minihan retired from active duty and the NSA directorship and was awarded the National Security Medal by President Clinton. (See Document B at end of chapter.) Two years earlier, he had written a note to the Agency workforce letting them know that the Cold War was "not decided on the battlefield, but won through vigilance and technology." The Cold War was marked by battles not fought and lives not lost. "We can all take pride," he wrote, "as intelligence professionals and Americans, in the role we played in securing peace for our country …"

Lieutenant General Hayden

NSA's Directors throughout the 1990s recognized the value of sharing the NSA success story with the American public. Directors and some senior NSA employees began meeting with both print and broadcast journalists and actively sought to identify unclassified NSA stories that could be openly shared.

One of most proactive Directors in this area was Lt Gen Michael V. Hayden, USAF. Appointed Director in February of 1999, Hayden would bring a wide range of experience to NSA, including tours as Air Attaché at the U.S. Embassy in Bulgaria and Director for Defense Policy and Arms Control at the National Security Council.

Like Lt Gen Minihan, Lt Gen Hayden served as Commander of the Air Intelligence Agency and Director of the Joint Command and Control Warfare Center. After his assignment as DIRNSA, Hayden left NSA to become the first Principal Deputy Director of National Intelligence, and later served as Director of the CIA.

At a speech at the American University in February 2000, Hayden acknowledged the public's legitimate privacy concerns in the new era of high-technology communications and noted that it was his goal to ensure that NSA worked with the appropriate judicial and legislative oversight authorities to protect American civil liberties.

In addition to his public appearances, Hayden engaged the press in unprecedented ways. Following the example set by General Minihan, Hayden actively reached out to the press, inviting journalists to his Fort Meade quarters for dinner and discussions on issues involving the Agency and its mission.

The terrorist attacks on September 11, 2001, brought this new openness to a temporary halt. While NSA continued to operate the National Cryptologic Museum, Hayden believed it was better to lower NSA's public profile during the immediate aftermath of the crisis.

Y2K

Worldwide concerns arose about the possibility of widespread system failures as the century clicked over from the 1900s to the 2000s. This problem was referred to as "Y2K." At NSA, computer programs and individual computers were diligently and thoroughly checked out months in advance to ensure that they would be able to handle the change to the new millennium. Each Agency component designated individuals who were to be on site or on call at the time of the millennial changeover.

With all the preparation, the Y2K problem ended up a non-event at NSA (and around the world). The Agency's methodical and well-documented approach to working through such a monumental task, however, set the stage for its work in the 21st century. ■

National Security Agency

Historic Documents

Document A – Memorandum from Vice Admiral William O. Studeman bidding farewell to the workforce

Document B – Presidential Memorandum awarding the National Security Medal to Lt Gen Minihan

DOCID: 3959496

Approved for Release by NSA on 03-09-2012, FOIA Case # 65724

UNITED STATES GOVERNMENT

memorandum

DATE: 8 April 1992

REPLY TO ATTN OF: DIRECTOR

SUBJECT: Farewell

TO: ALL EMPLOYEES

1. As time winds down on my nearly four years here at NSA as Director, I wanted to take the opportunity to thank everyone at the Agency and within the USSS for their kindnesses and professionalism. My wife Diane and I will miss you greatly, but we are filled with fond memories and impressions of the historical greatness of this powerful and magical institution. You have left me with some rich experiences which I hope to take into my new Community job, and in my new position, I hope to have continued interaction with NSA for the future.

2. One of the few legacies anyone can leave is to attempt to influence the succession. Admiral Mike McConnell is a magnificent intelligence officer, leader, and gentleman, and I know you will be well and effectively managed for the future. His tenure here will be filled with difficult conditions, and he will need all of your intellect, support and operational-technical innovation that you can muster.

3. Budget cuts and NSA's relative piece of the intelligence resource pie will likely diminish. Target technology will be tough, and many outsiders will want to rationalize a reduced threat dimension in order to further decrement intelligence for alternative agendas. There will be a trend to de-emphasize technical intelligence in favor of cheaper and historically less productive intelligence means.

4. To counter these factors, NSA must constantly demonstrate its operational and technical prowess to deliver in all business areas of intelligence, information systems security development and operation security training. We must be infinitely flexible and adaptable as well as effective, efficient and economical. We must manage our Community and partnership relations with great skill and aplomb. We must be seen to be responsive to our customer needs, and to reflect quality in every way, both internally and externally. We must plan and act out ahead of our targets and our business contemporaries. Investment for the future must be preserved at a high level, even at the expense of some other aspects of our resource base. We cannot be layered, inefficient, bureaucratic, top heavy, isolated, or turf minded. Increasing opportunities for duty outside NSA or overseas should be sought, and these people who go forth to broaden themselves should be understood

delivered to PCO on 920407 for distribution

42041

OPTIONAL FORM NO. 10 (REV. 1-80) GSA FPMR (41 CFR) 101-11.9 5010-114

Document A - Admiral Studeman bids farewell to the NSA workforce.

1523

THE WHITE HOUSE

WASHINGTON

March 17, 1999

4-29-99

ACTION

MEMORANDUM FOR THE PRESIDENT

FROM: SAMUEL BERGER for Kenneth D

SUBJECT: National Security Medal for NSA Director Minihan

Purpose

To secure your approval to award the National Security Medal to retiring National Security Agency Director Ken Minihan.

Background

George Tenet has nominated Lieutenant General Minihan to receive the National Security Medal.

During his 32-year military career, General Minihan has made a number of important contributions to our nation's security. As Director of NSA, he has worked tirelessly to ensure that our technical intelligence capabilities keep pace with a world that is changing rapidly both technologically and in terms of our security interests. His vision has been particularly instrumental in meeting the new challenges of the Information Age, specifically by developing new approaches for assuring the integrity of key national infrastructures. General Minihan retires this month.

RECOMMENDATION

That you approve the nomination of Lieutenant General Kenneth Minihan to receive the National Security Medal.

Approve _____

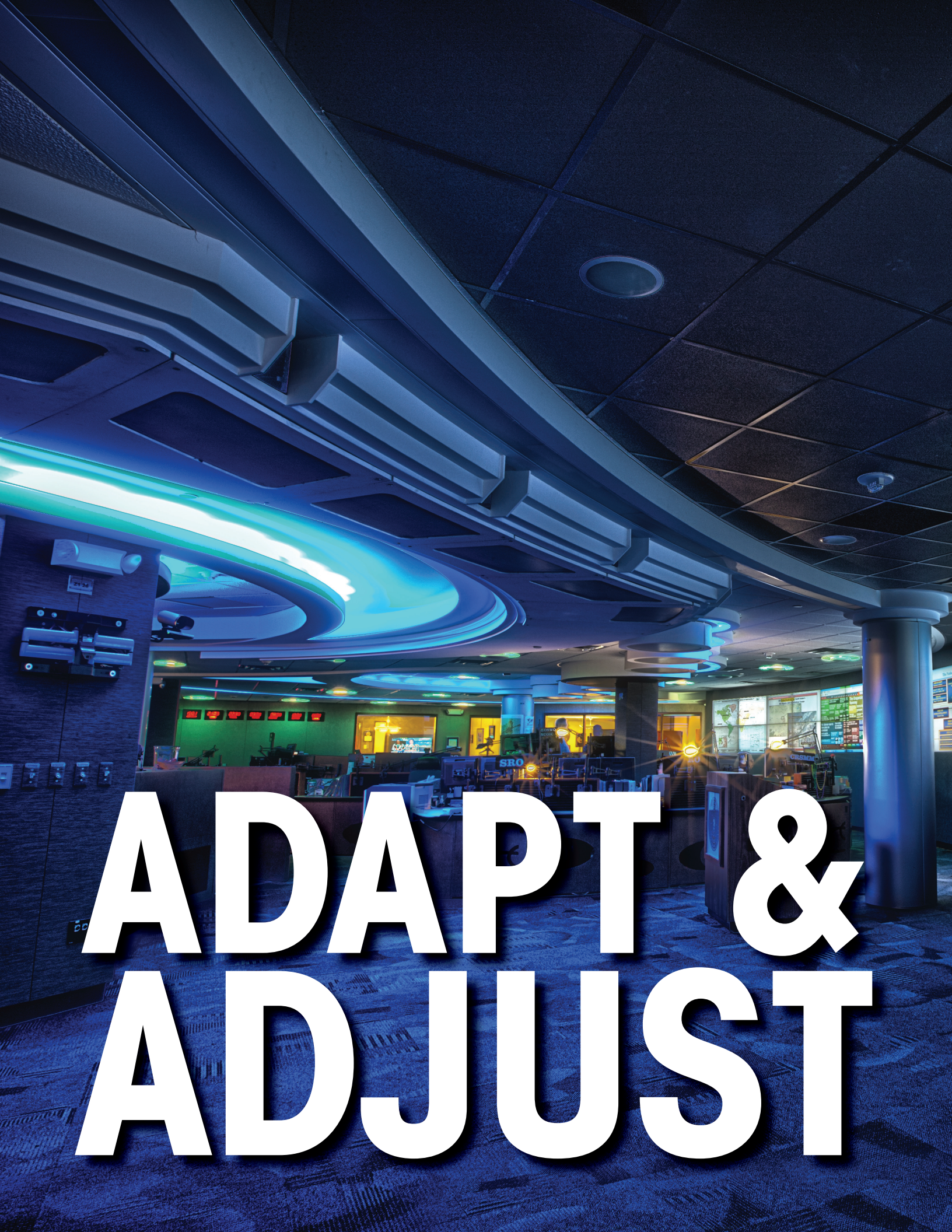
Disapprove _____

Attachment
Tab A Nomination Justification

cc: Vice President
Chief of Staff

CLINTON LIBRARY PHOTOCOPY
CLINTON LIBRARY PHOTOCOPY

Document B – Presidential Memorandum awarding the National Security Medal to Lt Gen Minihan, the first presentation of this medal by President Clinton.



ADAPT & ADJUST

2000s and beyond

The Information Age, begun in the 1990s, was now progressing to the point where technologies previously only dreamed of, were being developed and surpassed, and capabilities once available only to governments and businesses were now within reach of the general public.

For NSA, however, the great leaps forward were both a blessing and a curse. The Agency, like the rest of the intelligence and defense communities, benefitted immensely from the technologies brought about by the revolution in communications, but the need to keep pace could be daunting.

100 Days of Change

During the 1990s General Minihan encouraged the NSA workforce to embrace a new way of thinking about the cryptologic challenges of the future. General Hayden sought to accelerate these changes and implemented the new technologies available to assist the Agency in dealing with the challenges of the new century.

To accomplish these goals, General Hayden commissioned a study of NSA's organization and operations. He appointed two committees, one made up of in-house personnel and the other of cleared outsiders, and tasked them to make recommendations for change.

Based on their findings, in November 1999 Hayden instituted the "One Hundred Days of Change." As part of the new program, he issued a daily "DIRgram," a Director's message to the

View of the National Security Operations Center floor, 2012.

Director Hayden and 100 Days of Change.

NSA/CSS workforce, highlighting a different aspect of his transformation initiatives. (See Document A at end of chapter.)

The DIRgrams emphasized his basic themes of open communication up and down the chain of command and every employee's personal responsibility to foster beneficial change.

Among the changes implemented were:

- Creating a senior leadership team composed of the Director, Deputy Director, and the Directors of Signals Intelligence (SID), Information Assurance (IAD), and Technology (TD). (The other key component chiefs became associate directors and advisors to the senior leadership team.);
- Eliminating SID's internal divisions to speed reporting information and personnel shifts when crises arise;
- Hiring senior leaders from outside the Agency to address insularity, including the newly-created position of Chief Financial Officer. General Hayden also added a new position, Senior Acquisition Executive, to his leadership team;
- Holding Town Meetings to explain his policies and vision to the NSA workforce;
- Fostering working relationships with print and broadcast journalists by inviting them to unclassified sessions inside NSA;
- Eliminating most civilian promotion boards and returning authority for lower- and mid-level promotions to office supervisors.

In late February 2000, after 100 calendar days had passed since his program of change began, Hayden noted that, although some goals were still to be achieved, the "most important change of all" had occurred, namely, that employees and the Director were now "communicating freely, frequently, and clearly." Progress had been made, but all recognized more work needed to be done.

January 24, 2000

In the late 1990s and into the 21st century, media sources began to claim that NSA was falling behind in its adoption of modern communications and computer technology. The concerns proved to be valid. On January 24, 2000, a software anomaly caused a massive computer failure.

The outage was limited to the Fort Meade facility, but NSA processing systems were affected for 72 hours. Fortunately, there were no signs that the outage had been caused by malicious action or by an outside party. In addition, NSA was able to rely on other components of the cryptologic system to handle aspects of the mission that required immediate processing.

News of the outage leaked to the media, prompting General Hayden to go "on the record" with a broadcast journalist about the event. After service was restored, NSA issued a public

statement reassuring Americans that the Agency's essential activities had not suffered due to the outage and that no intelligence had been lost.

A New Approach

In July 2001 NSA announced the GROUNDBREAKER contract for technical support for much of its electronic infrastructure as part of the transition to greater reliance on contractor support. After a lengthy process of study and contract competition, a defense consortium and a few small technology companies were selected for the effort.

Contractors managed assets, such as desktop computers, telephones, and related equipment, freeing NSA technicians to concentrate on specialized operational equipment. As part of the program, incentives were offered to many of NSA's technical employees to move into the private sector. At the time, GROUNDBREAKER was the second largest U.S. Government information technology outsourcing effort ever. The program still exists today.

Interoperability

While technology was rapidly changing the SIGINT side of the mission, NSA's Information Assurance personnel were also working hard to improve the means of protecting information. One of the most impressive of these new developments was the creation of the Secure Terminal Equipment device or STE, which became the successor to the STU-III.

The STE was developed by IAD in partnership with private industry in the late 1990s to meet secure communications requirements raised by the DoD and other government agencies. Development began with a core version for offices with both digital ISDN (Integrated Services Digital Network) and analog PSTN (Public Switched Telephone Network) capabilities. Tactical, shipboard, and "data only" models would follow.

In 2000 the device was radically upgraded, and its modem was replaced with a commercial model. This new commercial technology

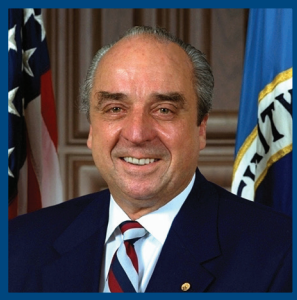
LEADERSHIP

DIRECTORS

Lt Gen Michael V. Hayden, USAF
(March 1999 – April 2005)

GEN Keith B. Alexander, USA
(August 2005 to Present)

DEPUTY DIRECTORS



William B. Black
(September 2000 - August 2006)

John C. "Chris" Inglis
(August 2006 - Present)

President Bush using a secure communication device on 9/11, reacting to World Trade Center bombing.

provided STE users with the interoperability needed to communicate with secure cell phones on the new digital cellular networks.

Most importantly for the future, the Secure Communications Interoperability Protocol (SCIP) built in the new devices provided secure operations among different devices, regardless of the actual communications system.

9/11

On September 11, 2001, America, NSA/CSS, and the world would be changed forever. The attacks that morning on the World Trade Centers and the Pentagon and the plane crash in Pennsylvania killed thousands of innocent citizens.

In the midst of the disaster, there arose a strong resolve among the Nation's leaders and its people to bring justice to those who had tried to brutally undermine the very foundations of American society.

Since the 1980s, NSA had been involved in counterterrorism efforts, but after the 9/11 attacks, NSA and the rest of the Nation would examine its readiness to deal with such an unconventional enemy.

"Something Was Imminent"

In the summer of 2001, NSA analysts working the terrorism target found more than 30 warnings that 'something was imminent,'

Aerial view of the damage to the Pentagon.

although none of the warnings contained specific information about targets or the timings of any planned attacks. Some analysts believed that the assassination of a major Afghan leader on September 10 might have been the event that these messages foretold.

Media reports stated that the day after the attacks NSA had published two reports that might have predicted the tragedies had they only been processed faster. The reality was that NSA had two pieces of intercept collected prior to September 11 that indicated that something of importance would happen on the 11th. However, these intercepts contained nothing beyond these vague hints – there were no details of expected action, time, or place that the U.S. could have acted on to prevent the attacks.

At a Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence on October 17, 2002, General Hayden stated for the record that, "Sadly, NSA had no SIGINT suggesting that al Qaeda was specifically targeting New York and Washington, D.C., or even that it was planning an attack on U.S. soil. Indeed, NSA had no knowledge before September 11th that any of the attackers were in the United States."

In June 2002, President George W. Bush visited NSA to show his support for its work and

Official USMC Photo
by Cpl Eric C Ely, 2D
Marine Division

Secure communications used by deployed forces in Iraq.

contribution in the war against terrorism. (See Document B at end of chapter.)

Afghanistan and Iraq

America's decision to carry the fight to Osama bin Laden and the Taliban on their territory was fraught with risk. American forces had to fight a new kind of war that depended on speed, technology, and accurate real-time intelligence; more than ever NSA was part of this fight. Even prior to the War on Terror, the Agency had begun to retool and revamp its operations to deal with the challenges of a new world driven by the need for continuous access to critical information and state-of-the-art technology.

As America's armed forces engaged the enemy in places like Afghanistan, the silent sentinels of NSA once again found themselves on the front lines of the conflict. The winning combination of innovative partnerships with local allies, as well as bravery, skill, and effective communications intelligence (both SIGINT and COMSEC) ousted the Taliban from power and dealt a stunning blow to bin Laden and the al Qaeda network.

During this effort, NSA and its Expeditionary SIGINT personnel ensured that diverse customers received the different types of products they needed. Whether the information was sent to the highest levels of military and civilian leadership or to the troops downrange, it was intelligence critical to achieving objectives and saving lives.

Likewise, NSA's Information Assurance personnel secured coalition networks and ensured secure communications for the warfighter. A corps of language analysts, cryptologists, technicians, and engineers and others supported the military of the

United States and its allies in missions throughout the battlespace.

NSA's strong commitment to serve the needs of U.S. military forces continued after the fall of Baghdad and after the defeat of the main Taliban forces. Indeed, as President Obama stated publicly, NSA was a key actor in the Special Forces-Intelligence Community team that finally brought bin Laden to justice in May 2011.

NSA's support of U.S. foreign policy goals was clearly evident in Operation IRAQI FREEDOM. SIGINT was a critical intelligence discipline relied on by U.S. and coalition forces in theater during the operation. NSA's investments in its global SIGINT architecture, connected with a distribution of NSA functions to Cryptologic Centers in Hawaii, Colorado, Texas, and Georgia, helped integrate SIGINT real-time support for battlefield commanders and gave strategic context for national-level policymakers. These innovations, articulated by Lieutenant General Keith B. Alexander, USA, who succeeded General Hayden as Director in 2005, also helped prompt changes in the overall strategy and priorities of the U.S. Intelligence Community.

Lieutenant General Alexander

General Alexander's ideas about how best to support the warfighter were influenced by his own combat experience in Operation DESERT STORM, as well as previous tours as Deputy Chief of Staff for Intelligence, U.S. Army, Commanding General of the Army Intelligence and Security Command, and Director of Intelligence at U.S. Central Command. In addition to his B.S. degree from the U.S. Military Academy, General Alexander holds Master's degrees in management, systems technology, physics, and national security from several prestigious academic institutions. General Alexander's educational and professional background enabled him to deal with the immense cryptologic challenges of the first decade of the 21st century.

General Alexander's innovative approaches to solving the challenges of the modern cryptologic mission resulted in his selection as the first Commander of the U.S. Cyber Command (USCC), and his promotion to the rank of four-star general. He retains his position as Director, NSA/Chief, CSS.

U.S. Cyber Command

General Alexander assumed command of USCC amid intense and growing national concern about developments in the cyber world. Given our society's dependence on digital networks and the growing number of threats to data and networks, cybersecurity was fast coming to dominate official and private agendas. This private and public attention only intensified as terrorist groups grew in their knowledge and use of digital technology, and as nations appeared to be behind some of the most worrisome cyber trends and incidents.

These concerns prompted several new tasks for NSA and drew extensively upon the Agency's expertise with all elements of cybersecurity. When the U.S. military reorganized its components for cyber operations in 2005, it based its new unit for "network warfare" at NSA and made the Director that component's Commander. NSA also contributed to then-President George W. Bush's government-wide Comprehensive National Cybersecurity Initiative, which was revised and expanded by President

General Keith B. Alexander, USA, Commander, CYBERCOM, Director NSA/Chief CSS

Barack Obama. When foreign intelligence malware infected U.S. military networks in 2008, NSA expertise played an critical role in Operation BUCKSHOT YANKEE, the network defenders' successful campaign to mitigate the computer security breach.

Secretary of Defense Robert Gates considered all of these experiences, and acknowledged NSA's expertise in the field, when he elected to co-locate Cyber Command with NSA at Fort Meade, and chose General Alexander as its first Commander. Although a separate Department of Defense organization, Cyber Command is able to leverage NSA's talented workforce, expertise, and record of innovation when necessary to accomplish its mission.

Looking Ahead

While future challenges and technical advances remain unknown, NSA must maintain a creative and versatile approach to its mission.

Today's most pressing threats include cyber terrorism, computer hacking, and debilitating computer viruses. Adversaries are constantly trying to steal America's digital information and compromise U.S. security. NSA protects both information and information technology that are essential to U.S. interests; defends critical U.S. and Allied networks against attack; and helps to identify and correct vulnerabilities in technology and operations. Together, these activities – providing information assurance and enabling computer network operations, along with the collection of foreign signals intelligence – form the core of NSA's mission.

NSA/CSS Threat Operations Center

In 2004 NSA Director General Hayden established the NSA/CSS Threat Operations Center (NTOC) as a joint Information Assurance and SIGINT initiative to assess and report on foreign threats against U.S. information systems. While NTOC's methods have changed and will continue to change with technology, its mission remains faithful to General Hayden's vision: "to look for new, creative, and collaborative ways to leverage our industrial-strength SIGINT and IA capabilities to live on the net always, shape the net sometimes, own the net when needed, and protect the net from those who wish to do the Nation harm."

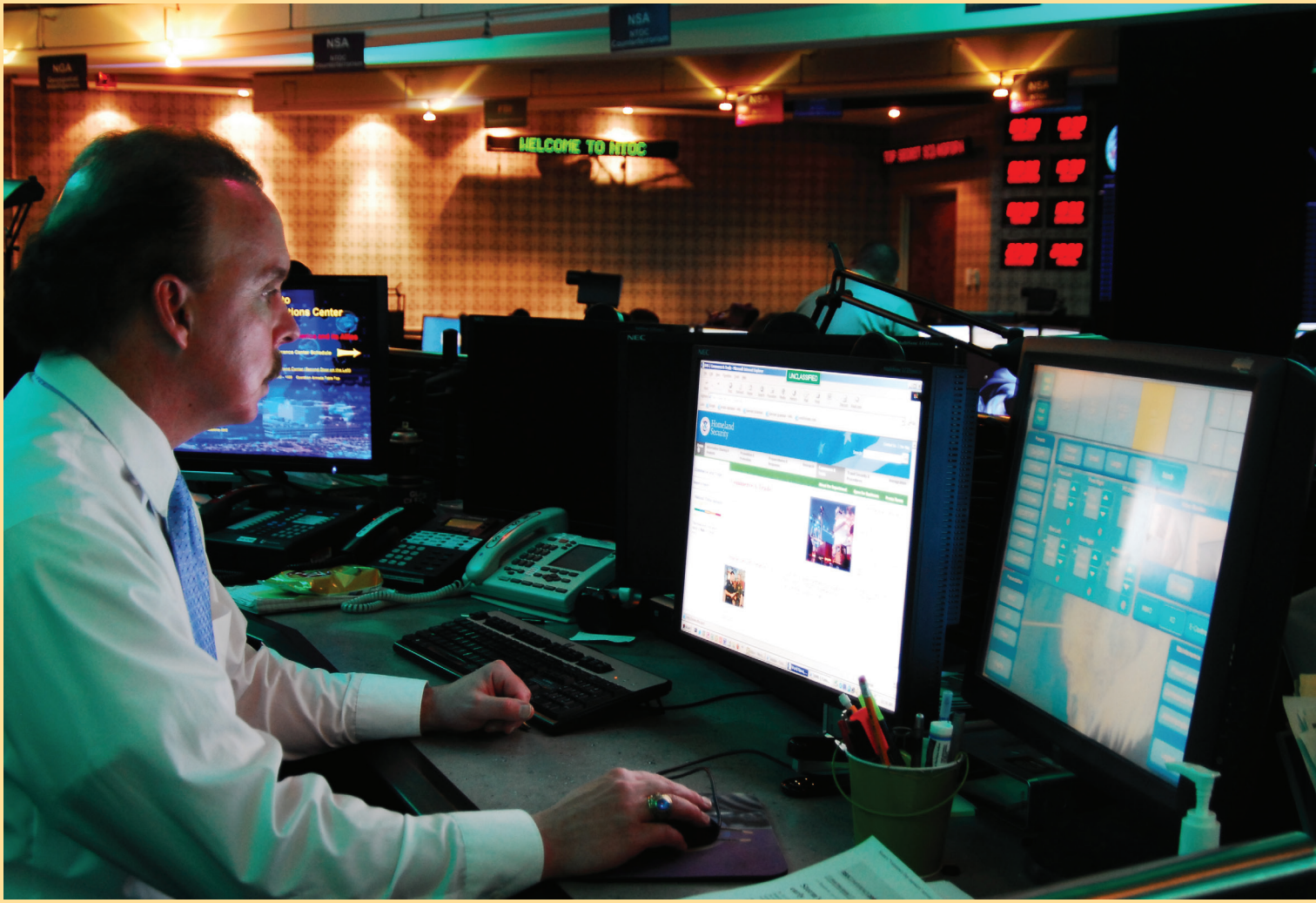
Recent world events and cyber's unprecedented growth necessitated a change in the way NTOC conducted this mission. In 2010 NTOC transformed its operations center into a more robust construct, providing maximum situational awareness of global network activities 24/7, 365 days a year.

Supporting Wireless Communications

The NSA Information Assurance Team has a long and successful history of customer engagement and industry collaboration to fulfill its responsibility for the security of National Security Systems. As the mobile market gained

momentum in the 1990s, NSA responded by working with the private sector to develop secure cell phones (CipherTAC-2000, Sectera-GSM and QSEC-800), as well as a secure modem to enable laptop access to SECRET networks. With increased commercial use of Personal Digital Assistants (PDAs), NSA developed the "Secure Mobile Environment Portable Electronic Device" (SME PED), a hand-held communication device with Type 1 encryption. This device provided secure voice and protected portable access to SECRET networks enabling customers to send and receive classified and unclassified voice calls as well as email and web browse on government networks.

In response to rapid technology and environmental changes, growing commercial use of Suite B cryptography, and increased customer expectations for consumer-like products, the Information Assurance Directorate initiated a significant two-pronged change to its business model. First, NSA renewed its engagement strategy with the private sector by updating and publishing a set of Protection Profiles for commercial products/technology to raise the level of security. Second, NSA shifted to a commercial technology first approach, moving away from building government-owned unique devices and infrastructure. Under this innovative process, called Commercial Solutions for Classified (CSfC), NSA supports the use of composed and layered secure standards-based commercial devices and services to create trusted devices and systems that can safeguard national security information and systems.



The NSA/CSS Threat Operations Center provides situational awareness on any adversarial attempt to exploit and attack our networks.

Secure Mobile Environment Portable Electronic Device.

The Mobility Mission Leader was appointed in 2009 and a Mobility Mission Management Office followed in the summer of 2010 to prove the value of implementing the CSfC model to deliver assured Mobility solutions. A matrixed NSA team created a highly successful pilot project using primarily commercial solutions to exchange secure voice and data on commercial mobile devices.

NSA will continue to innovate, test, and stay at the cutting edge of the mobility ecosystem to ensure anywhere, anytime access for classified government users and to influence the direction of security solutions throughout the federal government and in the private sector.

NSA's Public Perception

As the years passed and the environment changed, so too did the outlook of NSA's leadership, and once again NSA heightened its public profile. NSA's senior leadership can be seen giving high-profile presentations at technical conferences and events throughout the country, from General Alexander's first appearance at the 2009 RSA Conference to the Agency's participation in a documentary with the National Geographic channel.

For the first time since before 9/11, NSA allowed documentary cameras to go behind the closed doors of NSA and deep inside some of the Agency's watch center floors. "Inside the NSA" aired on the National

Geographic channel in January 2012 and featured interviews with NSA leaders and cryptologists about the Agency's critical role in protecting the country.

Hiring Boom

NSA's hiring efforts fluctuated over the last six decades as the demands on the Agency evolved. The '90s saw a decrease in hiring and a push for retirements. However, after 9/11, the trend reversed and the Agency was faced with the need to hire more professionals than ever in the Science, Technology, Engineering and Math (STEM) fields, foreign language, intelligence analysis, and others. In 2004 NSA began an effort to hire between 1,200 and 1,500 new employees a year for the next six years to meet the increasing demands placed on the ever-changing Intelligence Community.

In 2011 NSA took its hiring efforts into a new realm. To help recruit tech-savvy professionals to support the Agency's cyber security initiatives, NSA introduced several high-tech recruitment tools. These new digital communications – NSA Career Links Smartphone application, Crypto Mobile Game application, and Smartphone tagging – were designed to entice prospective employees to consider a career with NSA. Both 2011 and 2012 saw two of the largest hiring efforts in the Agency's history, with over 1,600 hires in 2011 and an expected 1,900 new employees in 2012.

Future Goals and Missions

The mission of NSA/CSS for 60 years has been to provide actionable Signals Intelligence to our customers, and to provide and protect the Nation's most important communications, all through the art and science of cryptology. NSA's activities, products, services, and information save lives and defend vital networks. To stay ahead of the Nation's adversaries, NSA is constantly adjusting and improving its capabilities to protect the Nation in this digital age. While technology, capabilities, and targets may change, NSA's core missions of Signals Intelligence and Information Assurance remain the same.

Centers of Academic Excellence

The "Centers of Excellence" program was started as a joint effort between NSA and the Department of Homeland Security (DHS) to reduce vulnerability in our national information infrastructure by promoting and cultivating interest in Information Assurance (IA). Educational institutions were invited to apply for NSA/DHS certification. The applications were evaluated on specific criteria about the faculty, coursework, and resources devoted to IA.

This focus on promoting IA at universities led to the development of more professionals in IA-related disciplines, as well as recognition for the school and scholarship and grant opportunities for students. In 2012 NSA and the DHS jointly sponsored several National Centers of Excellence in IA programs for four-year colleges, graduate-level universities, and some two-year colleges. NSA also launched a new National Centers of Academic Excellence in Cyber Operations Program to ultimately yield a larger pool of professionals with expertise in cyber security. ■

NSA Deputy Director John "Chris" Inglis swearing in new employees.

These missions will continue to enable us to discover our adversaries' secrets, while protecting our own, and to outmaneuver our adversaries in cyberspace, to provide our Nation the Information Advantage. General Alexander summarized his goals for the future in his Strategic Plan:

Goal 1: Succeeding in Today's Operations
Goal 2: Preparing for the Future
Goal 3: Enhancing and Leading an Expert Workforce
Goal 4: Implementing Best Business Practices
Goal 5: Manifesting Principled Performance

As General Alexander states in his foreword to the NSA/CSS Strategy, "Our success will be measured by how well we answer the Nation's key intelligence questions and how effectively we collaborate and integrate with consumers, partners, and others to help them achieve their missions, and protect and defend their information domains." ■

National Security Agency

Historic Documents

Document A – General Hayden DIRgram

Document B – President Bush's NSA address

DOCID: 2828030

(U) DIRgram-57: "100 Days of Change" Page 1 of 2

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Posted on: February 22, 2000

(U) DIRgram-57: "100 Days of Change"

Distribution: Director's Message to the Work Force

POC: Michael V. Hayden [talk_dirnsa@nsa]

Approved for Release by NSA on 11-18-2005, FOIA Case # 47501

(U) Today is the 100th calendar day since we began implementing the recommendations of the internal and external reports. Of the nearly five dozen DIRgrams I've published in the past 14 weeks, the ideas behind about a fifth of them didn't come from either report. They came from you, in the hundreds of e-mails you sent to me and the ENLIGHTEN postings you made. Partly because of your suggestions, and partly because some of the changes I wanted to begin in the first place still aren't quite ready to go, I'm going to keep putting out daily DIRgrams for two or three more weeks. Two of the biggest things still before us are:

- (U) getting our information technology infrastructure squared away, and

- (U) rolling out our business plan for 2000-2001 (particularly the major investments and operational shifts we're going to make, and the things we're ready to reduce or cut to pay for them).

(U) In some respects, I believe the most important change of all has already occurred: you and I are communicating freely, frequently, and clearly. These DIRgrams and your responses represent a tremendous change in the way information travels between us. Open communication is one of the most valuable things we can do to keep all of us moving forward together. Please keep writing.

(U) I promised you we would be unrelenting in changing NSA and CSS, and that what we begin, we will finish. I challenge those of you who have been "watching" our transformation so far to become active doers. To be sure this is more than words, I have commissioned an outreach effort directly to each of our first-level supervisors. We're doing it to ensure that all of our supervisors have a common understanding of my intent for our transformation, and that each has a good chance to discuss it with peers and provide me with fresh feedback and ideas. Most importantly, it will equip them to talk clearly with you about your personal role and responsibilities in building and shaping our common future.

MICHAEL V. HAYDEN
Lieutenant General, USAF
Director

http://www.n.nsa/cgi/agency-display.pl/20000222-070050 11/09/2005

Document A – DIRgram 57 from Lt Gen Hayden during implementation of his "100 Days of Change."

[Public Papers of the Presidents of the United States: George W. Bush (2006, Book I)]
[January 25, 2006]
[Pages 124-126]
[From the U.S. Government Printing Office www.gpo.gov]

Remarks Following a Visit to the National Security Agency at Fort Meade, Maryland
January 25, 2006

Thank you very much. I just had a really interesting visit here at the National Security Agency, and I want to thank General Alexander and all the folks who work out here for their hospitality and their briefing. I gave a speech to the men and women who are dedicating their lives to serving the American people and preventing this country from being attacked again. I was also able to talk to folks who work for the NSA, via video. They're around the world--some are in Iraq, some in Afghanistan. And it's just such an honor to be able to tell these people that the work they do is vital and necessary, and I support them 100 percent.

Most of the accomplishments, of course, that happen out here have got to be secret. But I know the good work they're doing. And so I want to assure the American people that we are lucky to have such professional, smart people working day and night to protect us.

The National Security Agency is playing a crucial part in the war on terror. First of all, the good folks who work out here understand we are at war, and they know what we know--that we face determined enemies who will strike without warning. And they know what I know, that we must learn the intentions of the enemies before they strike. That's what they do here--they work to protect us. The efforts of the people out here are a crucial part in protecting the homeland, and they've been a crucial

[[Page 125]]

part in success in Iraq and Afghanistan as well.

Officials here learn information about plotters and planners and people who would do us harm. Now, I understand there's some in America who say, ``Well, this can't be true--there are still people willing to attack.'' All I would ask them to do is listen to the words of Usama bin Laden and take him seriously. When he says he's going to hurt the American people again, or try to, he means it. I take it seriously, and the people of NSA take it seriously. And most of the American people take it seriously as well.

Part of the war on terror--we've seen that part of the terrorists' strategy is to place operatives inside of our country. They blend in with civilian population. They get their orders from overseas, and then they emerge to strike from within. We must be able to quickly detect when someone linked to Al Qaida is communicating with someone inside of America. That's one of the challenges of protecting the American people, and it's one of the lessons of September the 11th.

When terrorist operatives are here in America communicating with someone overseas, we must understand what's going on if we're going to do our job to protect the people. The safety and security of the American people depend on our ability to find out who the terrorists are talking to and what they're planning.

In the weeks following September the 11th, I authorized a terrorist surveillance program to detect and intercept Al Qaida communications involving someone here in the United States. This is a targeted program to intercept communications in which intelligence professionals have reason to believe that at least one person is a member or agent of Al

Document B-1 – Transcript of President George W. Bush's remarks during his visit to the National Security Agency, January 2006 (Full transcript and photographs available on DVD).

Qaida or a related terrorist organization. The program applies only to international communications. In other words, one end of the communication must be outside the United States.

We know that two of the hijackers who struck the Pentagon were inside the United States communicating with Al Qaida operatives overseas. But we didn't realize they were here plotting the attack until it was too late.

Here's what General Mike Hayden said--
he was the former Director here at NSA. He's now the Deputy Director of the National Intelligence--Deputy Director of National Intelligence--and here's what he said earlier this week: ``Had this program been in effect prior to 9/11, it is my professional judgment that we would have detected some of the 9/11 Al Qaida operatives in the United States, and we would have identified them as such.''

The 9/11 Commission made clear, in this era of new dangers, we must be able to connect the dots before the terrorists strike, so we can stop new attacks. And this NSA program is doing just that. General Hayden has confirmed that America has
gained information from this program that would not otherwise have been available. This information has helped prevent attacks and save American lives. This terrorist surveillance program includes multiple safeguards to protect civil liberties, and it is fully consistent with our Nation's laws and Constitution. Federal courts have consistently ruled that a President has authority under the Constitution to conduct foreign intelligence surveillance against our enemies.

My predecessors have used the same constitutional authority on numerous occasions. And the Supreme Court has ruled that Congress gave the President additional authority to use the traditional tools--or ``fundamental incidents''--of war in the fight against terror when Congress passed the authorization for the use of military force in 2001. These tools include surveillance to detect and prevent further attacks by our enemies. I have the authority, both from the Constitution and the Congress, to undertake this vital program. The American people expect me to protect their lives

[[Page 126]]

and their civil liberties, and that's exactly what we're doing with this program.

I'll continue to reauthorize this program for so long as our country faces a continuing threat from Al Qaida and related groups. This enemy still wants to do harm to the American people. We cannot let the fact that we have not been attacked lull us into the illusion that the threats to our Nation have disappeared. They have not disappeared; the terrorists are still active. And we've seen their activity in London and Madrid and Bali and Beslan and Amman and Baghdad and many other places since September the 11th. Just last week, as I mentioned earlier, we heard from Usama bin Laden. The terrorists
will do everything they can to strike us. And I'm going to continue to do everything I can within my legal authority to stop them, and so are the good people here at NSA.

In the long run, we can be confident in the outcome of this struggle, because we've seen the power of freedom to defeat tyranny and terror before. And we can be confident because we know our military and law enforcement and homeland security and intelligence professionals are working day and night to protect us.

I'm grateful for the skill and dedication of the good folks who work out here. These are fine patriots, and they're making America safer. Thank you all very much.

Note: The President spoke at 2:10 p.m. In his remarks, he referred to

Document B-2

An Agency Rich in Heritage

Secrecy and a Low Profile

From the moment an employee is hired on at NSA, he or she assumes a lifetime obligation to safeguard sensitive and classified information. Every new employee is educated in the need and requirement for secrecy, as well as the importance of keeping a low profile on the "outside" for counterintelligence reasons.

Gradually, however, the philosophy that produced the expression "NSA means No Such Agency" has morphed into one of more openness. An iconic symbol of this transformation is the signpost reading "The National Security Agency" that was placed at its entrance in the 1990s.

Although the obligation for secrets to remain secret has not changed, NSA has both a physical presence and a virtual one. The topic of a recent National Geographic documentary, NSA also has its own web page, its Director speaks at approximately 40 external events yearly, and its actions are followed, not always accurately, in the daily press.

Early NSA Newsletter..

Dress Code

In the early days, NSA had a dress code that mandated business attire for all employees. Coat and tie were required for men and conventional business dress for women, which did not include pantsuits.

In the 1960s, as fashion in society became less formal, dress codes were relaxed for both civilians and military. Eventually, many formal fashion practices, such as neckties, were abandoned by almost everyone but senior leaders.

In the 2000s, employees dressed based on their function and the needs of the office. Leadership adopted the attitude that what was in an employee's head was more important than what was on the body.

Smoking

Reflecting the norms of society, smoking was widespread throughout the Agency in the early days, with ashtrays a common sight on many desks. As the general public became more aware of the dangers of smoking, NSA followed suit and began to work to adopt a smoke-free environment.

In February 1989, Director Studeman signed a memorandum prohibiting smoking in all offices, limiting its use to designated areas in the cafeteria. This partial ban lasted till the end of the year, when Studeman ordered that NSA be totally smoke-free by 1 January 1990.

Alcohol

One of the most intriguing NSA cultural facts was the presence of beer machines in the cafeteria in the '70s and '80s. Eventually, the beer machines were removed, although the story lingers as an interesting piece of trivia.

Work-Life Balance

By the late 1990s, NSA leaders and the Human Resources organizations established several programs to help employees achieve a healthy

Winners of the Miss NSA contest, circa 1960s.

work-life balance. Today NSA's leadership is aware that a "whole person" –someone with balance between their professional and personal sides of life– can contribute more substantially to the mission.

Job Diversification

In the early years, it was not unusual for an employee to spend an entire career in a single office or career field. By the 2000s, at least one tour of duty or joint duty assignment at another intelligence agency or military command would be a prerequisite for high-level promotions.

Publications

Employees in the early years, bound by NSA's policy of anonymity outside the Agency, were discouraged from publishing articles in academic or popular journals. Consequently, NSA established a number of in-house journals, such as the NSA Technical Journal, established in 1956, and Cryptologic Spectrum, which started in 1969. These two publications were combined in 1982 as Cryptologic Quarterly, which is still published today.

In 1953 the Agency began publishing a simple four-page newsletter, which was replaced in 1964 with a slicker version, the NSA Newsletter. This paper ceased publication in 2000.

Activities

Over the years, NSA has sanctioned a number of after-hours activities and sports leagues, like softball and bowling. There were also clubs for handicrafts, travel, skiing, and games, and an art guild that exhibited members' work. For a time, there was a clown club and a drama club. NSA personnel also formed many types of music groups, including the Parkway Brass and Parkway Chorale, who frequently perform at the Agency.

NSA's talented Parkway Chorale performs at many high-profile events.

2012 Armed Forces Week 5K Race

In 1970 Admiral Gayler approved the formation of the Phoenix Society, intended for NSA retirees to help prolong friendships and interests developed over the course of a career at NSA.

NSA has also sponsored "learned societies," such as the Crypto-Linguistic Association, the CryptoMath Institute, the Pen and Cursor Society, and the International Affairs Institute.

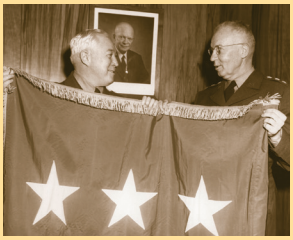
The Workforce

NSA Deputy Director John "Chris" Inglis sums up the NSA workforce in this quote, "Remarkable people with remarkable skills form the heart of the National Security Agency."

Many factors, while they have evolved over the last 60 years, combine to create a diverse and stimulating environment that fosters a rich and rewarding career. The challenges of aggressively taking on an adversary or resolutely protecting the home turf bring out the best in people. The commitment and dedication of Agency personnel is one key factor that has not changed over the years. NSA employees are dedicated, bright, loyal and serve the Nation in silence. ■

NSA Timeline • 1952 to 2012

1952
LTG Canine
NSA's first Director established a strong foundation for the fledgling organization.



1960
Martin & Mitchell The defection of these NSA employees to the Soviet Union prompted tighter personnel security measures.

1962
Cuban Missile Crisis SIGINT played a critical role in defusing this event that had the world on edge.

1972
Central Security Service (CSS)
The CSS established a full partnership between NSA and the Cryptologic elements of the Armed Forces.

1975
Lt Gen Allen
During his tenure, Gen Allen faced the Church Committee's investigation into NSA collection practices.

1950 1960 1970 1980

1952
VENONA
The VENONA project exposed a massive Soviet espionage effort that threatened national security.

1962
Specialist James Davis killed in combat in Vietnam
The first Soldier killed was an advisor to a South Vietnamese Radio Research unit.

1957
The move to Ft. Meade
One reason the site was selected was because it was deemed far enough away from the capital in case of a nuclear strike.

1974
Deputy Director Tordella
Dr. Tordella, who served as DDIR for 16 years, was an early advocate of the use of computers in cryptology.

1986
President Reagan President Reagan, accompanied by Mrs. Reagan, dedicated NSA's Operations 2A and 2B buildings.

1991
Desert Storm NSA provided key SIGINT support during this conflict.

1993
National Crytologic Museum The Museum tells the story of the important role that cryptology has played throughout history.

1999
Lt Gen Hayden 100 Days of Change This initiative encouraged free, frequent, and clear communications up and down the chain of command.

2001
9/11 Attacks On this day, NSA, America, and the world changed forever.

2011
Bin Laden brought to justice NSA was a key actor in the Special Forces-IC Team responsible for this action.

1990 2000 2010

1985
The Year of the Spy Former NSA employee Ronald Pelton and Petty Officer John Walker were convicted of espionage.

1996
National Vigilance Park The Park features three aircraft used in aerial reconnaissance missions.

2003
Afghanistan & Iraq NSA's strong commitment to serve the needs of the U.S. military was and is evident in both conflicts.

2010
GEN Alexander & U.S. CYBERCOM Gen Alexander was promoted to the rank of four star general and named Commander, U.S. Cyber Command in 2010.

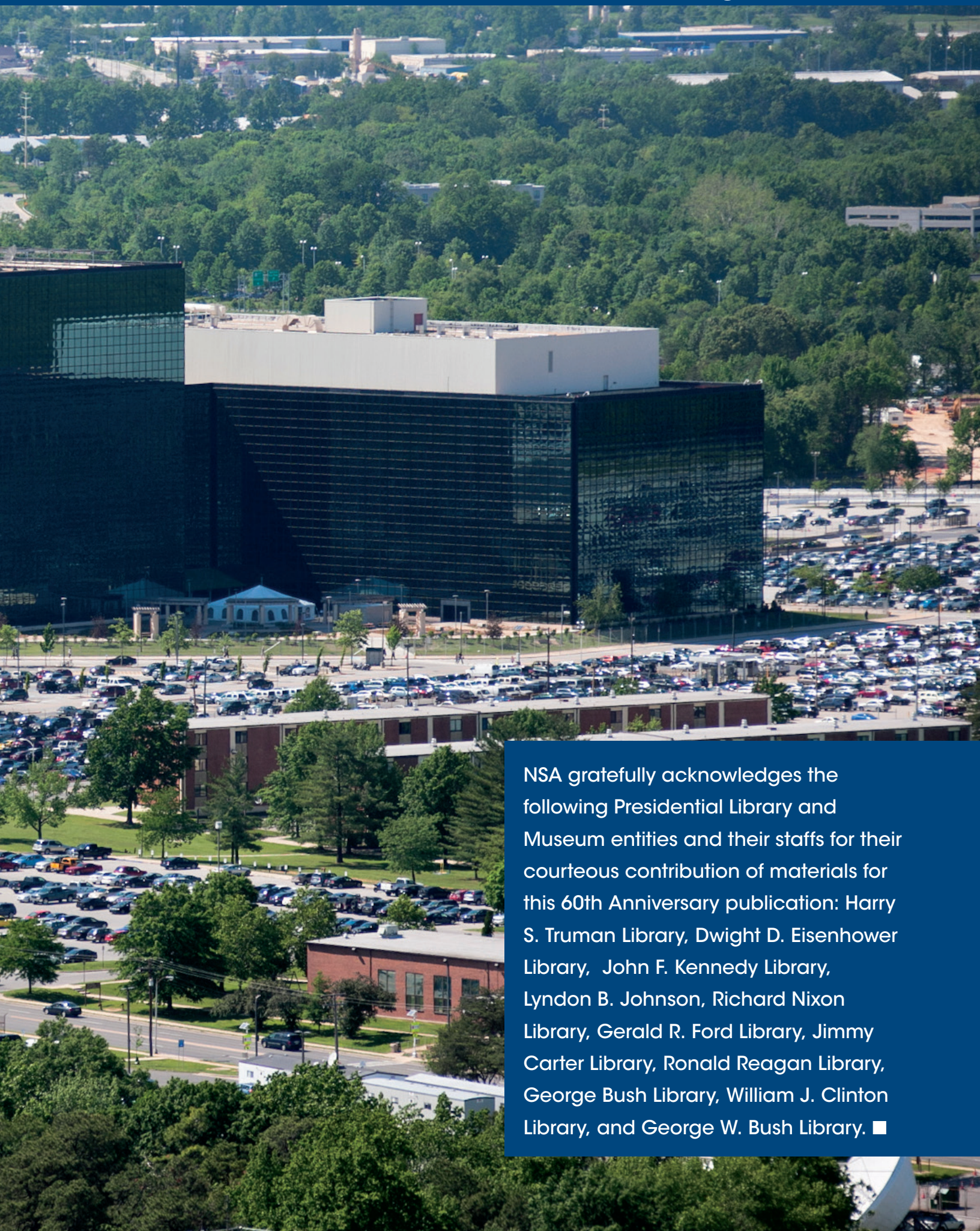
National Security Agency

The NSA seal is a circle with a white border. In the semicircle border are the words National Security Agency and United States of America, separated by a five-point silver star. In a blue field, an American eagle is displayed with wings inverted and talons clutching a silver key. On the breast of the eagle is a shield, with a blue top, supported by thirteen red and white stripes. In heraldry, the eagle is a symbol of courage, supreme power, and authority. The eagle in the NSA symbol symbolizes the national scope of the mission of the Agency. A description of the shield taken from the Great Seal of the United States explains that the shield "represents the several states all joined in one solid compact entire, supporting a chief, which unites the whole and represents Congress." The key in the eagle's talons, representing the key to security, evolves from the emblem of St. Peter the Apostle and his power to loose and to bind. The shape of the seal, a circle, represents perpetuity of its continuance, the symbol of eternity. ■

Central Security Service

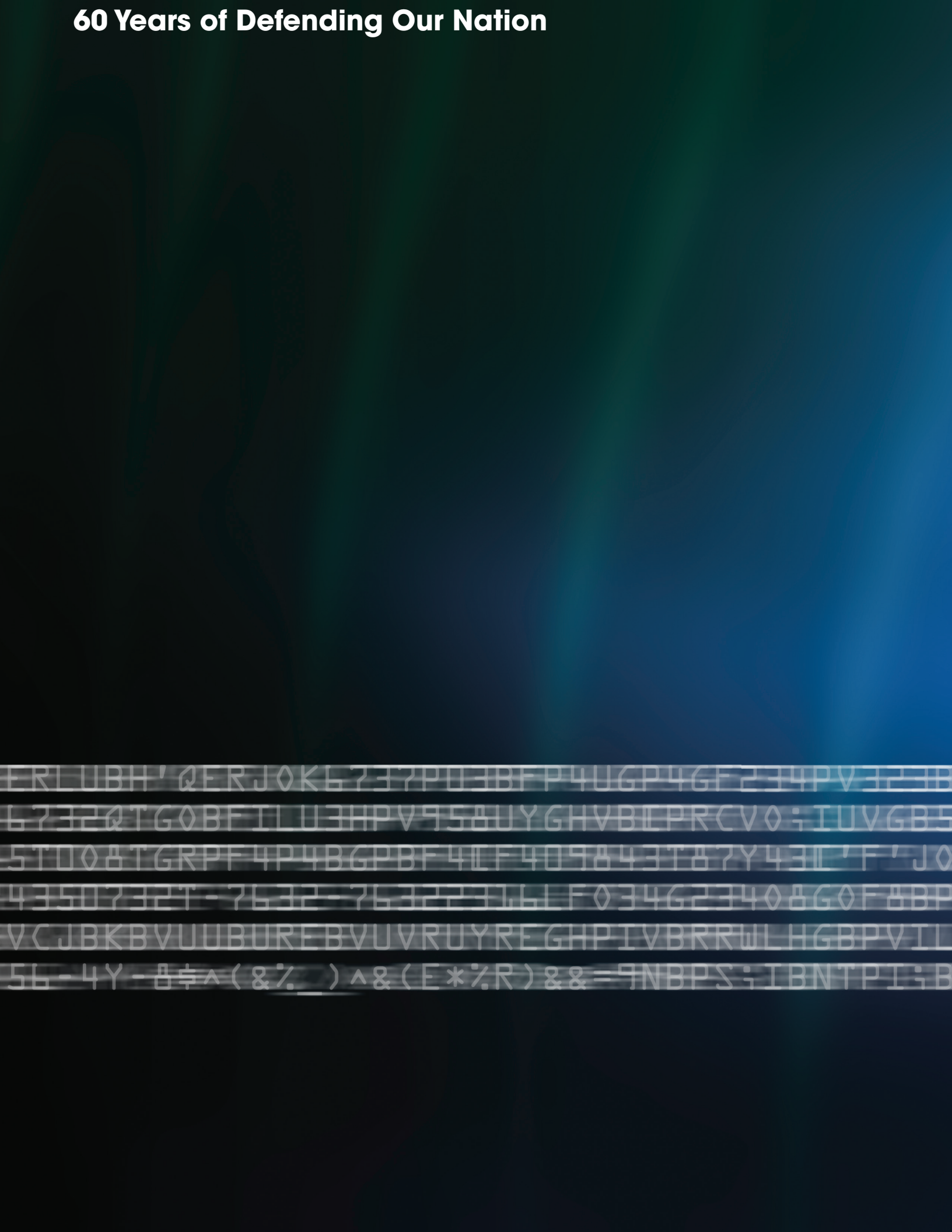
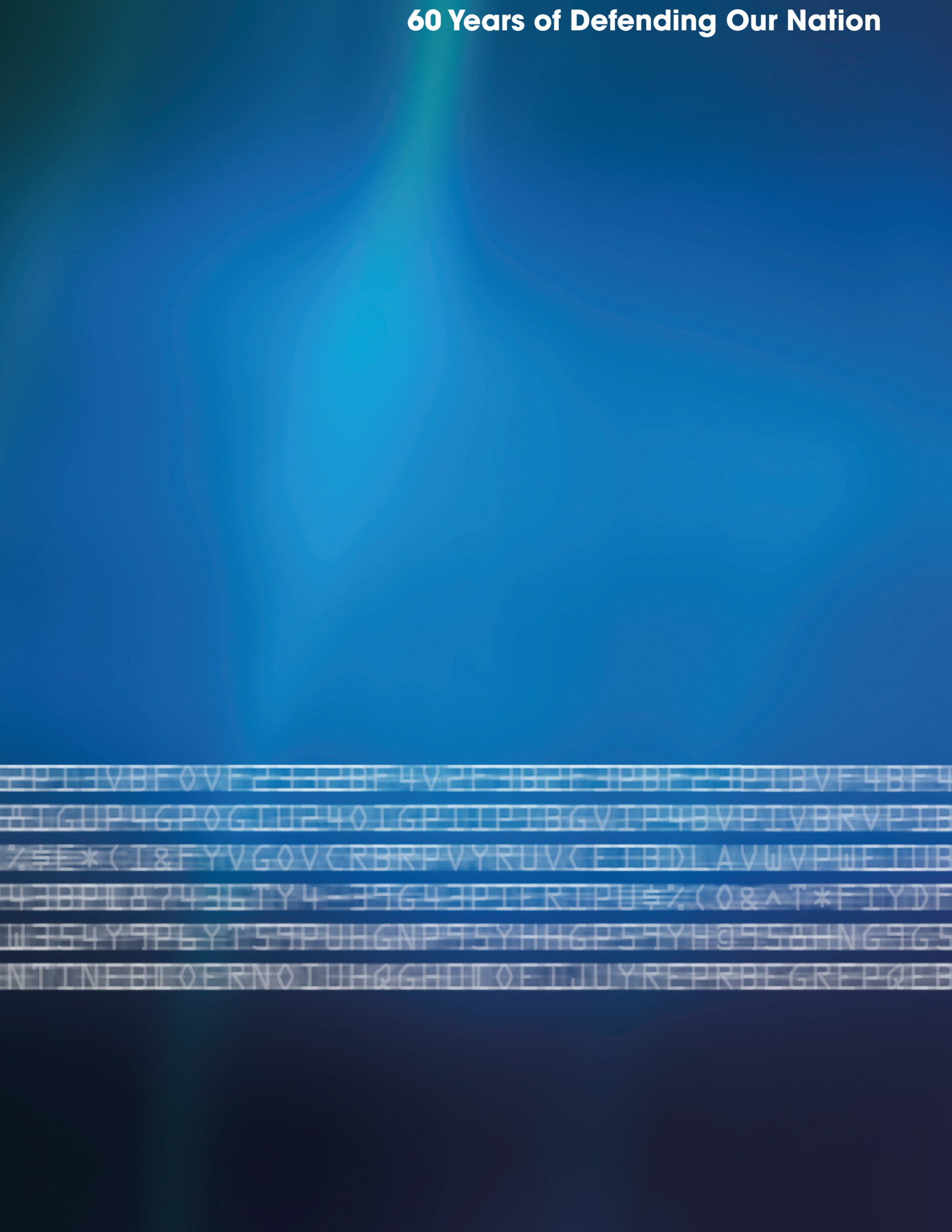
The CSS seal displays all five Service Cryptologic Components, which are comprised of the United States Fleet Cyber Command, the United States Marine Corps Director of Intelligence, the United States Army's Intelligence and Security Command, the United States Air Force's Intelligence, Surveillance, and Reconnaissance Agency, and the United States Coast Guard Deputy Assistant Commandant for Intelligence. Each are equally balanced around a five point star on which is centered the symbol of NSA/CSS, which provides the funding, direction, and guidance to all of America's SIGINT activities. ■

60 Years of Defending Our Nation



NSA gratefully acknowledges the following Presidential Library and Museum entities and their staffs for their courteous contribution of materials for this 60th Anniversary publication: Harry S. Truman Library, Dwight D. Eisenhower Library, John F. Kennedy Library, Lyndon B. Johnson, Richard Nixon Library, Gerald R. Ford Library, Jimmy Carter Library, Ronald Reagan Library, George Bush Library, William J. Clinton Library, and George W. Bush Library. ■

60 Years of Defending Our Nation



60 Years of Defending Our Nation