The Link

BULLETIN OF THE NATIONAL CRYPTOLOGIC MUSEUM FOUNDATION, INC.

VOLUME 6, NUMBER 1 Spring 2003

NATIONAL SECURITY AGENCY HALL OF HONOR

With appropriate fanfare, NSA Director Lt. Gen. Michael V. Hayden, USAF, unveiled the latest additions to NSA's Hall of Honor at the National Cryptologic Museum on 12 June 2003. Four names have been added to the 21 honored since 1999, when the first eight "inductees" were selected to inaugurate the Hall. They are the late Lambros D. Callimahos, aide to the legendary William F. Friedman and guru of a generation of cryptanalysts; mathematician Dr. Lowell K. Frazer, a leader in the arcane field of cryptographic evaluation; Mrs. Juanita M. Moody, whose years of experience as an analyst culminated in her leadership role during the Cuban Missile Crisis and the subsequent re-shaping of NSA's SIGINT reporting and representation; and the late Howard E. Rosenblum, an electronic engineer and senior manager, whose work centered on secure speech encryption.

After opening remarks by NCM Curator Jack E. Ingram and welcome by Gen. Hayden, honorees or family representatives joined the Director for the unveiling of plaques, as the NSA Historian, Dr. David A. Hatch, read the supporting narratives for the new inductees. (See inside, page 3.) The National Cryptologic Museum Foundation hosted a reception following the ceremony.

IN THIS ISSUE

Continued on page 3

OVERVIEW

It had been a number of years since I was inside a public school. But this April I visited several schools participating in our "a[ll] k[ids] a[re] SMART" program and saw for myself the excitement and enthusiasm evident among both students and educators. Excitement and enthusiasm over learning math? Yes, when the ingredients of computers, a "treasure-hunting" incentive, and competition are combined, as they are in the program initiated by CPL and enabled by NCMF "seed money." The concept, sketched in the Winter Issue of *The Link*, has caught on, as you'll see in the accompanying article from the Annapolis newspaper, and other school jurisdictions have asked how they can "join." Already our colleagues are looking beyond mathematics to developing comparable programs for foreign languages or other fields in which cryptology and national security share common interests...and seeking the public sector funding sources to enable the program to continue and to expand.

As I said last quarter, recommendations of our Ad Hoc Committee on Board Structure and Composition are being implemented. You may note on the back page that several new names have been added to the Board of Directors – former NSA Director Lincoln D. "Linc" Faurer (Lt. Gen. USAF, Ret.), and former NSA officials , MG Thomas J. Flynn (USA Ret.), and Mr. Michael J. Jacobs and Mr. William J. Geiger. They bring fresh talent and enthusiasm to our ranks, and we heartily welcome them. Fred Demech has had to step down as our PAO (after a fine record of performance) and Dr. Sally Botsai has taken the helm of that important post.

On the other hand, it seems only yesterday that we welcomed Betty Ferrone to our ranks; now we have had to bid her goodbye – for the time. It seems that NSA had need for her abilities and experience and have asked her to rejoin the Agency workforce. (And they pay better, I'm afraid.) We are so pleased with this recognition of qualities that attracted her to the NCMF and wish her every success. Now we're seeking someone to share office time with Sherri – a part-time, but a compensated, position.

It was gratifying to receive a significant donation from Eagle Alliance, resulting from this year's golf tournament. We'll save that story for the next issue, when we should have some pictures of the presentation and new information about the tournament.

While we were not able to have this year's General Membership Meeting and the biennial Cryptologic History Symposium coincide, both will take place "off campus," the latter at the Maritime Institute near Baltimore in October. The Foundation has been asked to assist the Center for Cyptologic History (CCH) with some of the supporting actions for the symposium, and we are pleased to be able to offer that assistance.

John E. Morrison, Jr.
President

HELP WANTED!!

As with most non-profit, volunteer organizations, the NCMF needs willing hands as well as financial support to achieve its objectives of supporting the present NCM and building toward a world-class facility in the future. There always seems to be a need for help and an open invitation stands ready to those who would bring fresh ideas to our attention – volunteers who relish the opportunity to renew or continue their association with the unique people and things associated with cryptology. These are volunteer jobs – or, as some like to say, their payment comes in another form than money.

Most of these opportunities are with one of the following committees: Acquisition, Development, Educational, Facilities, Finance and Audit, Membership Programs, Public Affairs, and Recognition. If any of these subject activities interest you, or you would like more information on the functions of any of these Committees please call us at the office, (301) 688-5436, email us at cryptmf@aol.com, or send us a note at: The NCMF, P. O. Box 1682, Ft. George G. Meade, Maryland 20755-9998.

A specific immediate need is with the Acquisition Committee which has the responsibility of acquiring artifacts for display in the museum. Individuals interested in the material culture of cryptologic history should find serving on this Committee a rewarding experience.

HALL OF HONOR

Continued from page 1

LAMBROS D. CALLIMAHOS was born December 16, 1910, in Alexandria, Egypt, of Greek parents and came to the United States at age four. When college age, he attended Rutgers University to study law, but transferred to Julliard, from which he graduated in 1933. After a few years of concert touring as a flutist, Mr. Callimahos, an avid amateur cryptologist, joined the U.S. Army in 1941 and entered the cryptologic service.

After basic training, Mr. Callimahos taught cryptanalysis and Italian at the language department at Fort Monmouth. He graduated from Officers Training School in 1942 and was supposed to spend the next several months developing a new cryptologic course with William Friedman. However, a chain of changes led to his enrollment in a Japanese course and subsequent assignment to New Delhi as assistant signals intelligence officer for the China-Burma-India Theater. When the war was over, he was finally assigned to the Army Security Agency as Friedman's assistant.

Through the 1950s, Mr. Callimahos collaborated with Friedman on a variety of projects and developed his own famous class, CA-400. This was an expansion of Friedman's original intensive-study senior cryptanalytic course. Mr. Callimahos taught 32 sessions of CA-400, for a total of 270 students. Graduates of CA-400, the elite among cryptanalysts, became members of the Dundee Society and played crucial roles in shaping cryptologic development at NSA.

A prolific writer of cryptologic literature, he was the author of over forty books, monographs, and articles. He helped establish NSA's Technical Journal in 1955 and served as technical advisor to the publication for the rest of his career. He wrote articles on codes and ciphers for numerous reference works, including Encyclopedia Britannica.

By the end of his career, Mr. Callimahos was respected by his colleagues and students as a true Renaissance man: teacher, writer, linguist, cryptologist, and flutist. He was awarded the NSA Exceptional Civilian Service Award on 24 August 1976. Illness forced him to retire in late 1976.

Lambros Callimahos died on October 28, 1977.

DR. LOWELL K. ("JIM") FRAZER founded modern cryptographic evaluation. As a result of his efforts, all cryptography used for classified applications by the U.S. Department of Defense and intelligence community is now subject to rigorous scientific evaluation. He influenced the design of most U.S. cryptographic systems fielded before 1990. In addition, Dr. Frazer was a prolific writer of technical papers.

His college career at Indiana University was interrupted by World War II; he received his Ph.D. in 1951. Shortly after, Dr. Frazer went to work for what is now NSA.

He was selected as the first COMSEC mathematician assigned as an integrated member at GCHQ from 1954 to 1956. During this two-year tour, he performed assessments on many cryptographic systems, designed speech cryptosystems, and discovered an analytic technique that would be widely used over the next three decades. Also, he authored a training primer for new COMSEC cryptomathematicians.

Dr. Frazer was the principal formulator of standards the U.S. and the U.K. use to judge the strength of cryptographic systems. He continued to lead the adaptation and extension of those standards as the role of cryptography grew from COMSEC to a more diverse mission.

Under his leadership, the industrial TEMPEST program, a novel approach to government-industry interaction, matured. The program integrated TEMPEST concerns into the security evaluation process for U. S. cryptographic equipment.

Dr. Frazer played a major role in developing NSA's mathematics, cryptanalysis, and Information Assurance communities. He assisted in developing

Continued on page 4

HALL OF HONOR

Continued from page 3

the National Cryptologic School and was associated with the CryptoMath Institute from its inception. He was a member of the Mathematics, Cryptanalysis, and COMSEC Career Panels, and was an advisor to the NSA Technical Journal for approximately twenty years.

Dr. Frazer received numerous awards throughout his career, including the Agency's Meritorious Civilian Service Award in 1969, the Exceptional Civilian Service Award in 1981, and the DCI's National Intelligence Distinguished Service Medal in 1985.

Dr. Frazer was born 15 May 1925 in Mt. Liberty (now Nashville), Indiana. He currently resides in Florida.

Recalling the Cuban Missile Crisis of 1962, former NSA senior JUANITA MOODY said that it "allowed us to take advantage of everything we had learned during World War II and post-World War II . . .and I felt that every day in my career in the Agency from the Cuban crisis on was affected by my experience at that time."

In early 1943 Juanita Morris, attending a small college in North Carolina, wished to contribute to the war effort and volunteered at the nearest recruiting office. By April, Juanita Morris was at the Army cryptologic headquarters at Arlington Hall Station. While she was awaiting her security clearance, the SSA put her into unclassified training in cryptanalysis; she became fascinated with the subject.

At the end of the war, her supervisor asked her to stay on, rather than be demobilized, and she agreed. In 1948 she married Warren Moody, a non-cryptologic employee.

Ms. Moody supervised NSA's day-to-day – sometimes minute-by-minute – response to the Cuban Missile Crisis as head of the major element responsible for SIGINT on that region. In addition to directing production and reporting, she frequently gave impromptu briefings to high-level civilian and military leaders. She often worked around the clock, grabbing only a few hours' sleep on a cot in her office.

In the years following the Cuban Missile Crisis, Ms. Moody was assigned to higher positions within the production organization at NSA. She revolutionized SIGINT reporting, and put NSA into the White House Situation Room. After thirty-three years of service Ms. Moody decided to retire in 1976.

The previous December she had become the first recipient of the National Foreign Intelligence Medal of Achievement, presented by then Director of Central Intelligence George H. W. Bush.

Ms. Moody currently resides in South Carolina.

HOWARD E. ROSENBLUM probably had as much effect on the development, application, and fielding of secure speech equipment as any other single person in the post-World War II communication security (COMSEC) community in the United States.

He graduated from the City College of New York in 1950 with a BSEE and immediately went to work for the Department of Defense at the Naval Research Laboratory. In 1953 he came to NSA and worked in Research and Development, specializing in COMSEC design. After some field assignments and short stints with contracting firms, Mr. Rosenblum returned to NSA in 1962. He headed the Secure Speech Division that was designing a series of early vocoder systems meant to secure both strategic and tactical government and military speech communications.

On the tactical side, Mr. Rosenblum's division developed and fielded secure speech equipment for short-range military field radios such as the KY-8 (NESTOR). This equipment was needed urgently by U.S. forces in Vietnam to provide security against an opponent fully capable of exploiting unprotected U.S. communications.

Mr. Rosenblum's research division was responsible for the conceptualization and design of follow-on secure speech systems that are prevalent today. His division's research into digital conversion

Continued on page 5

HALL OF HONOR

Continued from page 4

allowed for development of the Secure Telephone Unit (STU) family of systems used throughout the federal government. Mr. Rosenblum personally was responsible for developing the concept of the key distribution center that enabled any user to establish individually secure telephone calls within the network of STU users. In 1983 Mr. Rosenblum was awarded a patent for the concept of the key distribution center.

In 1971 Mr. Rosenblum was appointed director of Research and Engineering. From 1978 to his retirement in 1983, he was deputy director for Communication Security. In 1971 he received the NSA Exceptional Civilian Service Award, NSA's highest civilian award.

Mr. Rosenblum was born 28 April 1928 in Brooklyn, New York. He passed away 8 October 1996.

COMING EVENTS

Keep yourself posted on coming events and changes beyond the scope of *The Link* by marking and regularly re-visiting the NCMF and NSA web sites. Here, for calendar-marking purposes, are planned forthcoming events that may interest you:

12 September 2003 (All Day)
Fifth Annual NCMF General Membership meeting
Location: To be announced

This year's theme is Homeland Security. We plan to invite a senior official of the new department as our keynoter.

20-21 September 2003
Eisenhower Historic Site, Gettysburg, PA 17325

Over 100 living history enthusiasts will portray military personnel from the European Theater of Operations. Programs presented will include W.W. II medical services, weapons and equipment, communications, military vehicles, tanks, and the life of the common GI. (We understand that the Navy cryptologists of 1941-42 *may* be featured at 1100 Sunday.) This is a National Park Service, paid-

Continued on page 8

THROUGH KGB EYES

Another highly successful NCMF program was held on 24 April, featuring two former Soviet KGB senior officers, MG Oleg Kalugin and COL Val Aksilenko. COL Aksilenko offered perspectives of the Al Qaeda master plan, tying 9/11 and other terrorist events world wide with strategy to create a Muslim state in Central Asia. COL Aksilenko's experience in negotiating safe passage for Soviet troops and material out of Afghanistan gives him unique insight into the personalities of the region and their long term objectives.

MG Kalugin spoke eloquently on US-Russian relations under Russian President Putin. His personal knowledge and professional relationship over the years with now President Putin provided fascinating views of the challenges Russian leadership faces both domestically and internationally.

Not too many years ago, face-to-face encounters of this type between cloistered NSA employees and their KGB counterparts would have been beyond the wildest imagination. Old habits (and NDAs) die hard, even when one of the two contending powers no longer exists as such. A feeling of constraint still prevails in such gatherings, but it was an unforgettable experience for the fully engaged audience. By agreement with the speakers, this program was not video-taped. See what you missed?

(Left to Right) Aksilenko, Morrison, Kalugin

NATIONAL HISTORY COMPETITIONS

National History Day and Maryland Day are year-long education programs that make history come alive through education, professional development and active student learning. The NCMF supports these programs with monetary prizes and recognition for work related to the field of cyptology, cryptologic history, and national security interests.

We awarded two prizes in cryptology at the statewide Maryland History Day competition on 26 April 2003.

Lindsey Comer's paper, "National Security and the Public Rights" won in the junior division. Lindsey attends Elkridge Landing Middle School in Howard County. Her teacher is Mr. Doug Jones. Ashley Barbera, a student at Liberty High School in Carroll County won the prize in the senior division. Her paper was entitled "Spying on the Spies: A Look into the Rights and Responsibilities of the Intelligence Community." Ms. Christine Cohn and Mr. Ed DeVincent are her teachers.

Two other Maryland History Day projects related to intelligence advanced to the National History Day competition: "The Pentagon Papers – Rights and Responsibilities: National Security and the First Amendment", a documentary completed by Emily Hoffman of Plum Point Middle School in Calvert County and Zack Sandberg's performance "I Spy or Should I? The Congressional Oversight of the CIA". Zack is a student at Eastern Middle School in Montgomery County. The National History Day competition was held 15-19 June at the University of Maryland College Park – results in the next issue.

Congratulations to all.

As we did last year, we will be seeking permission to add the papers and projects to the National Cryptologic Museum's library.

THE LEWIS & CLARK EXPEDITION

It was perhaps natural that a CIA employee with an interest in history would first draw the Editor's attention to the military and "classified" nature of the 1803 expedition now drawing international attention. President Thomas Jefferson's known interest in anthropology, geography, and other fields of science afforded plausible reasons for launching an exploratory expedition into the newly acquired far western land of the Louisiana Purchase. But why charge two army officers with the task? Why provide them with a platoon of soldiers and the most modern weapons available from the government arsenal at Harper's Ferry? Jefferson's "plausible reasons" and innocent scientific curiosity could also be considered suitable cover, to use the modern term, for an extended reconnaissance into unknown country, seeking to ferret out potential schemes and designs of the British, French and Spanish in the area. An *intelligence* mission, conceived and tasked directly by the President/Commander-in-Chief. This lends another aspect to the "Corps of Discovery."

This thought came to mind last year, when it was learned that Mr. Jefferson's friends at Monticello had determined not to be left out in 2003. They noted that Jefferson's young friend and confidential secretary, Meriwether Lewis (captain of infantry, U.S. Army), had been invited to Monticello for detailed discussion and instruction. Monticello, they successfully argued, should be the easternmost site associated with the commemoration of the anniversary. And so it was.

But what does this have to do with the field of cryptology? Simply put, a covert mission (even one with good plausible cover) needs some provision for private, confidential communication "back to headquarters" – a cipher, a secret code. And sure enough, that was part of Jefferson's equipment for the mission: he evidently provided the leaders a variant of the hoary "Vigenère" cipher (also known as the

Continued on page 11

"BREAKING THE CODES"
KIDS HAVE FUN WITH GAMES THAT HELP TEACH MATH SKILLS

by Kimberly Marselas - photos by Andy Carruthers

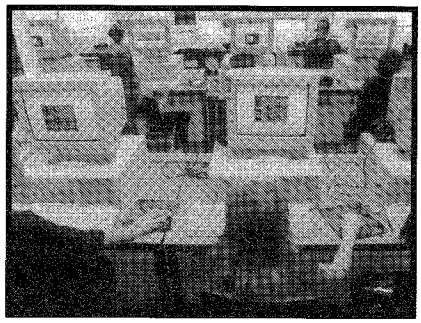
(Reprinted by permission from "The Capital," Annapolis, Maryland. A related article appeared in "The Baltimore Sun" 14 June 2003)

It's just after noon when code-breaker Daniel Haller enters the computer lab, takes a seat and calls up a private log-in screen for secret agents.

Trying not to draw any attention, he quietly types in his password and focuses on the jumble of numbers that begin flitting across his monitor.

Then he moves his Harry Potter lunchbox out of the way and gets down to the real work: figuring out how to make a three-by-three block of varying numbers add up to the same amount in every direction.

The Linthicum Elementary School third-grader is one of about 150 county students participating in a.k.a. Smart, a series of code-breaking challenges designed to get children interested in math careers.



Linthicum Elementary School students tackle a variety of code-breaking and logic games. The group is participating in the pilot of a code-breaking program.

The eight-week pilot program was developed by the National Cryptologic Museum Foundation and began at Linthicum, Corkran Middle and Severna Park High schools in March.

The espionage-tinged festivities will end Friday when the youngest students get a final crack at a complex code.

The program is voluntary, and it's held during recess at the elementary school level.

Fourth-grader Bobby Cone said he was willing to give up two outdoor play sessions each week "because the games are challenging, sometimes fun, and sometimes frustrating."

That was the goal, said Morrie Cove, whose Cipher Limited Partnership Co. is working with the museum foundation to fine-tune and expand the program.

All of the 40 or so math games and logic puzzles used by the a.k.a. Smart students can be tailored to their grade level and the local curriculum.

For example, cryptograms like the one fifth-grader Christiana Sabett solved yesterday can be coordinated with classroom lessons on long division or basic geometry.

Cryptograms, in which students replace one letter with another to uncover a phrase, are one of the Linthicum group's favorite games.

"I like the challenge of finding out what the words are and then trying to do it faster," said Christiana, zooming onto another puzzle before the 30-minute session ended.

"This is really fun."

All around the computer lab, students showed their enthusiasm for math during yesterday's sessions. Some stared open-mouthed at their screens, trying to break through a math barrier. Others yelled "Yes, I won!" or shouted "Sweet!" when they discovered a new game during their final round of tournament style play.

Middle and high schoolers have been equally enthusiastic, participating after school and logging on to the Web-based program from their homes.

"The high school kids were reluctant at first," said Patty Kneisly, a gifted and talented coordinator who oversees the program for the school system. "But once we got them into the computer lab, into the program, then they got hooked on the games."

Mr. Cove is hoping a.k.a. Smart will expand to 15 or 20 schools next year – it may remain in Anne Arundel schools as well – and eventually become a national competition complete with cash prizes, university scholarships and internship opportunities.

"All kids, even some adults, today are intoxicated by computers," Mr. Cove said. "We want to turn that into a long-term interest in math."

To the far left: Fourth-grader Bobby Cone is engrossed in a tile-stacking game in which he must unearth matching pieces from the bottom of a 3-D pile. The Linthicum Elementary School student is one of nearly 150 county children participating in the pilot of a code-breaking program sponsored by the National Cryptologic Museum Foundation. Left: Volunteer Bernie Farkas helps third-graders Shane Smith, front, and Ninlola Oyinloye work on a game where they have to realign a series of geometric jewels in under 30 minutes.

HAPPY 68TH BIRTHDAY, NAVAL SECURITY GROUP

by CAPT Kathleen B. Nelson
(Reprinted by permission from "Anchor Watch," NSGA Fort Meade, Maryland, and the Summer issue of "Cryptolog.")

The primary reason we study history is to learn from our past – to avoid previous mistakes and to repeat and improve on our successes. The Naval Security Group celebrated its birthday on March 11th, so it is an appropriate time to reflect on the lessons and inspirations of our cryptologic heritage.

Since at least 1917, cryptologic duties have been performed in the Navy. From 1924 to 1935, the Naval cryptologic service developed operationally, resulting in the formation of the Naval Security Group on March 11, 1935. In SECGRU's early days, dedicated enlisted Sailors and officers trained themselves in our core cyptologic disciplines and were instrumental in providing intelligence supporting major campaigns during World War II.

Each year we remember the contributions of our predecessors, members of the "On-the-Roof" Gang, by recognizing the accomplishments of current Naval cryptologists with an award given in their name. From 1928 - 1941 150 Sailors and 26 Marines perfected their communications intelligence on the roof of the old Main Navy Building in Washington, D.C. The "On-the-Roof" gang awards are presented each year at the Naval Cryptologic Veterans Association annual convention where active Navy and Marine cyptologists can meet and swap sea stories with cryptologic veterans.

Our role hasn't changed significantly in the last 68 years. As cryptologists we use every technology available to provide intelligence in support of Navy war fighters. Our purpose is to support Naval and national operations that ensure the defense of the United States. Technology and equipment have changed, field sites around the world have come and gone, but the business of defending the nation is the same. We are recognized experts in our field, and the last career cryptologic force in the military services. Navy operational commanders have come to rely on our particular expertise in signals analysis, cryptolinguistics, communications intelligence, information security, and now computer network defense and information operations.

The Navy and Naval Security Group are transforming but like cryptologists before us, we continue to seek creative solutions to intelligence gaps, have developed and modified equipment to specialized operational tasks, served alongside Sailors wherever Naval forces have deployed to ensure their safety and support their operational success.

So, be proud of your Naval cryptologic heritage and recognize that you represent the Naval Security Group, the Navy, and all those men and women who served before you–Sailors and Marines whose contributions turned the tide in times of war, including the Battle of Midway and helped to maintain the peace during the Cold War. Take advantage of every opportunity you have to improve your technical skills, to increase your rating knowledge, and to serve alongside the very operational forces we are tasked to support. Be ready for the unique challenges our new adversaries present, because the one constant we can count on is being called to serve wherever and whenever the Navy is engaged.

Captain Kathleen B. Nelson, commanding officer USNSGA, Fort Meade, Maryland

COMING EVENTS

Continued from page 5

admission event. (No NCMF involvement.) Adults - $7.00, Children (13 to 16) $4.00, Children (6 to 12) $2.50. Golden Age passport holders $4.00. Visit http://www.nps.gov/eise/enhsce.htm for details.

30 - 31 October 2003 (All Day)
Ninth Cryptologic History Symposium
Maritime Institute, Linthicum, Maryland

NSA's Center for Cryptologic History has announced its Ninth Cryptologic History Symposium, unclassified and open to the public. Visit www.nsa.gov or e-mail the CCH Technical Director, Dr. David Hatch, at dahatch@nsa.gov if you have not received an invitation and desire to attend.

3 December 2003, 4-6 p.m.
Location to be announced in the invitation

This will be the third in our annual series on cryptology and the WWII War in the Pacific. We'll update in the next issue of *The Link*, or check the NCMF web site.

FAREWELL TO THE NAVY WULLENWEBERS

by Al Grobmeier

(Reprinted from the U.S. Naval Cryptologic Veterans Association "Cryptolog," Summer 2003)

In the early 1960s the U.S. Navy built 14 AN/FRD-10 Wullenweber Circularly Disposed Antenna Arrays/Circular Dipole Antenna Arrays (CDAA) on established Navy installations at the following locations: Most lasted into the late 1990s. First built was Hanza in 1962, last built was Imperial Beach in 1964, and first to be dismantled was Marietta in 1972.

Pacific Area: Adak, Alaska, Marietta, Washington, Skaggs Island, California, Imperial Beach, California, Wahiawa, Hawaii, Guam, Mariana Islands, and Hanza, Okinawa, Japan

Atlantic Area: Winter Harbor, Maine, Northwest, Virginia, Homestead, Florida, Sabana Seca, Puerto Rico, Galeta Island, Panama, Edzell, Scotland, and Rota, Spain

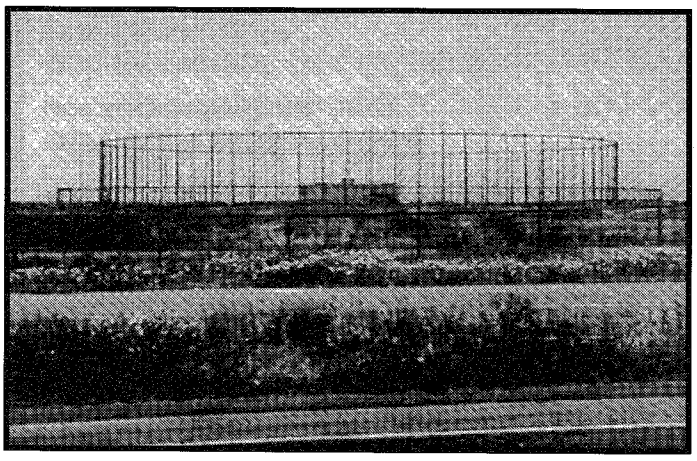
In addition, two CDAAs were built side-by-side for general service ship-shore communications at Sugar Grove, West Virginia.

Of the above 16 CDAAs only the following remain standing at the locations indicated, all others having been removed: 1) Naval Computer and Telecommunications Area Master Station Pacific, Wahiawa, Hawaii. 2) Former Naval Radio Receiving Facility, Imperial Beach, California. The disposition of the entire site is under discussion. The site is presently under control of the Naval Special Warfare Command and the CDAA area is used as a storage lot for SPAWAR vehicles. It was proposed that demolition of the CDAA be accomplished in-house by the Navy but for safety reasons that was abandoned and no further plans have emerged. 3) Former Naval Security Group Activity, Galeta Island, Panama. When the U.S. gave the site to Panama, all equipment was removed and only the CDAA and ops building remained. The Panamanian Government gave the site to the Panamanian Technological Institute, but there has been no current use of the site. It is being guarded by a group of police to prevent looting and vandalism. The antenna is not being maintained and there are a couple of places where the CDAA has fallen.

The present status as given for all 16 CDAAs has been confirmed except the removal of the Sabana Seca CDAA. It was severely damaged in a hurricane in 1998 and was not repaired. It is presumed that it has now been removed since the base was closed as of 31 January 2003.

The University of Illinois' developmental Wullenweber antenna south of Bondville, Illinois was abandoned about 1980 and has now (2003) been completely dismantled.

It should be noted that the U.S. Air force and U.S. Army had several AN/FLR-9 CDAAs at overseas bases where the Navy was a tenant including Alaska, Philippines, Japan, Germany and Italy. Canada operated two AN/FRD-10 CDAAs, at Masset, British Columbia and at Gander, Newfoundland. Likewise, the Navy maintained a miniature Wullenweber CDAA AN/AX-16 Pusher at Diego Garcia, BIOT.



Imperial Beach CDAA. Photo taken from the east, facing west. The CDAA site originally contained WWII wooden buildings of the old "intercept station 1"

U.S. NAVY PHONETICS

Curiosity over the designation, CAST, for the early WWII Navy station on Corrigidor ("The Link," Winter 2002) prompted us to turn to our colleague, Ray Schmidt, who responded as follows:

Phonetic Alphabets and Names for Early Navy Cryptologic Stations

Raymond P. Schmidt

When it absolutely, Positively Must Get There Ungarbled!

Throughout history, communications among navy units during combat needed to be short, crisp, and to the point. "Sighted Sub, Sank Same" purportedly sent by a Navy pilot in World War II serves to illustrate these critical qualities of signals that date back to even earlier days.

Brevity and clarity were only two of the imperatives that governed naval communications, of course. At times, speed and security also became essential, but either of the latter could sometimes be emphasized or sacrificed as determined by the operational commander. The essence of the message, on the other hand, could never be compromised. "When in doubt, mumble" went nowhere in becoming official naval communications doctrine. (You can test this as a general premise by considering requirements for communicating with your spouse, children, friends, business associates, or the teller at your bank.)

Whether messages prior to the invention of computers were sent *en clair* or encrypted, however, the need for precision in understanding was paramount. The use of signal flags and pennants established this principle, and the introduction of Morse code and voice transmissions in the 20th century highlighted a compelling requirement to eliminate ambiguity.

One means of enhancing understanding was to ensure that letters of the alphabet were not mistaken for one another. It made a difference if the letter was "B" rather than "E" or "M" and not "N" – even though they could easily sound the same. Thus, a need to prevent garbles helped stimulate development of a phonetic alphabet to identify letters being sent via radio or telephone landline – or in Morse code. Both the United States Navy and the Army employed such lists of words even before World War I. These phonetic alphabets were used primarily to avoid garbled meanings.

The Navy Phonetic Alphabet

An early version of the Navy phonetic alphabet appeared in 1913 using some familiar words that lasted through World War II: "Able" for A and "Fox" for F. Other words disappeared after World War I and never showed up again: "Boy" for B, "Have" for H, "Pup" for P, "Rush" for R, and "Watch" for W. Several words were temporarily replaced, but later came back into use during World War II: "Item" for I, "Nan" for N, and "Oboe" for O. A few curious words even lasted until 1927, but then disappeared forever: "Quack" for Q and "Vice" for V.

The second version of an official alphabet was adopted in 1927, and a third slight variation came into use in 1938. With a few tweaks, that third alphabet became the one familiar to students of World War II history, and fans of popular films of that era know about such terms as "Baker Company" and "Checkpoint Charlie." All but five of the Navy words used in World War II were identical with Army and Allied phonetic alphabet words.

The fifth and current alphabet was adopted in 1957, retaining only four of the World War II words. For Navy signalmen, the early phonetic alphabet was paired with the Alphabetical Code Flags defined in the International Code. The meanings of the flags and their names were selected by international agreement. In time, that listing also included the Morse code signal.

Using the Phonetic Alphabet as Shorthand for Navy Stations

Prosaic uses for phonetic alphabet words developed as officials assigned letters of the alphabet to buildings and even geographic sites. These soon assumed an identity of their own.

For those concerned with U.S. naval cyptologic history, a relative handful of words became important during the interwar years as the shorthand names of shore stations: "BAKER" for Guam in the Marina Islands, "CAST" for Mariveles [later, Cavite and then Corregidor in the Philippine Islands], "HYPO" for Heeia in Hawaii, and "NEGAT" for the Navy Department in Washington. Perhaps the first, but less often mentioned, was Station "A" ("AFFIRM") located in Shanghai in China. Station "D" ("DOG") was unique: It moved because it was on board the Asiatic Fleet flagship.

To succeeding generations, the origins of the names for early stations faded and may even generate an aura of mystery. With the rapid expansion brought about by the war after 1941, shorthand names for

Continued on page 11

U.S. NAVY PHONETICS

Continued from page 10

stations underwent significant changes. At some point, the phonetic alphabet handles were dropped and "USN-" designators came into use. But for the several hundred Navy personnel engaged in radio intelligence prior to the attack on Pearl Harbor, the phonetic alphabet names served a small but vital organization.

Captain Schmidt was ordered to Key West, Florida at the height of the Cuban Missile Crisis in October 1962 where he served as communications officer for the Naval Security Group Detachment and Activity. He later served as the first naval cryptologic historian in a civilian capacity from 1968 until 1981, and speaks several phonetic alphabets fluently.

FOR THE BOOKSHELF

(The April issue of the quarterly journal, "Cryptologia," contains the following book review by editor (and NCMF member) Lou Kruh, reprinted here by permission.)

C.G. McKay and Bengt Beckman, *Swedish Signal Intelligence 1900-1945*. Portland, Oregon: Frank Cass Publishers, 2003.

"The authors present a definitive account of the evolution of Swedish signal intelligence between 1900 and 1945 based on an exhaustive study of official archives. It is an interesting and surprisingly revealing source of European cryptology in the first half of the twentieth century, with many examples of how ciphers were solved. There are fascinating glimpses into the development of Swedish intelligence contacts, with accounts of Swedish-German cryptanalytical cooperation during World War I in intercepting and solving Russian diplomatic telegram traffic. There is also an authoritative account of Swedish success against German and Soviet traffic during World War II. Further insights are gained when McKay and Beckman describe the remarkable Swedish large-scale solution of German diplomatic telegram intercepts, Russian naval and military traffic, and those of other nations in the 1939-1945 period.

"This history provides new insights to the development of cipher machines by Siemens and Halske, Lorenz, L.M. Ericsson, and others, including the Aktiebolaget Cryptograph Company and the important Hagelin firm. Its first major technical contribution was the B-21, a rotor machine produced for the Swedish General Staff in 1925 and during World War II, its C-38 became the M-209 when used by the United States in 1942. The authors also shed light on the transfer of the Finnish intelligence services to Sweden in 1944 and show how MI5 (British Security Service) had someone at work in the Swedish Legation in London. The outstanding work of well known cryptanalysts such as Yves Glydén, Arne Beurling, who solved German *Geheimschreiber* messages, and others are also described.

"This excellent book is an authoritative account that belongs in your personal library."

[Note: Co-author Bengt Beckman was identified in ***Cryptologia****, XXVI #2, April 2002, "An Early Cipher Device: Fredrik Gripenstierna's Machine," as a retired official from Sweden's counterpart of NSA, the National Defense Radio Establishment. – Ed.]*

THE LEWIS & CLARK EXPEDITION

Continued from page 6

"court" or "diplomatic" cipher). The 26 x 26 alphabet square, well known to cryptologists, lacks a provision for Arabic numerals – all numbers must be "spelled out" or left "in the clear." Mr. Jefferson aimed to remedy that, and he did so, with a 27 x 26 matrix (he included the ampersand, &) and provision for enciphering numerals 1-0. (A photograph of his manuscript from the Library of Congress appears as Figure 29 in Silvio A. Bedini's 1990 *Thomas Jefferson: Statesman of Science.* The cipher is WE 065 in Ralph E. Weber's 1979 *United States Diplomatic Codes and Ciphers*, 1775-1938, using "antipodes" as the keyword in the example. It is similar to WE 066 and to WE 096, suggested to Jefferson by Oliver Wolcott in 1795.)

And so, as Monticello argued a role in the ongoing commemoration of the expedition, we also argue, on behalf of the shades of American cryptographers past, that a memory of the event has a home at the National Cryptologic Museum through our cryptography-minded third President.

Join the National Cryptologic Museum Foundation

ANNUAL MEMBERSHIP APPLICATION

❑ Please begin/renew my membership in the Foundation

❑ Benefactor $10,000	❑ Patron $5,000
❑ Sponsor $1,000	❑ Donor $500
❑ Supporter $250	❑ Contributor $100
❑ Sustainer $50	❑ Member $25

The Foundation is certified as a non-profit organization by the I.R.S.

Name _____

Address _____

City _____

State _____ Zip _____

Phone _____ E-Mail _____

Date _____

Please make your check payable to:

The National Cryptologic Museum Foundation

The National Cryptologic Museum Foundation, Inc.

CONTACT US:
(301) 688-5436 & 5437
Fax (301) 688-5619
email: cryptmf@aol.com
http://www.nationalcryptologicmuseumfoundation.com

MUSEUM TELEPHONE:
(301) 688-5849

MUSEUM HOURS:
Monday - Friday - 9:00 a.m. - 4:00 p.m.
1st & 3rd Saturdays - 10:00 a.m. - 2:00 p.m.