The Spyglass

United States Naval Criminal Investigative Service

Volume II

Edition 7

December 1998

Fighting Computer Crime

Computer Investigations and Operations Department

December 1998

On the Cover - *Fighting crime in the "Information Age" requires training and resources, which is why the Computer Investigations and Operations (CIO) Department has become a priority for NCIS. To find out more about how NCIS is responding to "cyber crime," see the article beginning on page 2.*

Director David L. Brant

Deputy Director John F. McEleny

Assistant Director for
Government Liaison & Public Affairs
Special Agent Victor H. McPherson

Deputy Assistant Director for
Congressional Liaison & Public Affairs
Mr. Thomas F. Houston

Editor: *Gary M. Comerford*
Assistant Editor: *YNC Sherri Jones, USNR*

Editorial Assistants

Larry Welch
YN3 Roseanne Sambuco, USNR
Shelia Reeves

The articles used on the front cover were reprinted with the permission of ***Federal Computer Week***.

This edition of the *NCIS Bulletin* was published with administrative assistance from Naval Reserve Unit NCISHQ 0166.

Director's Message . . .

Director Brant and the Nance family

When Gerry Nance retired a few weeks ago, one of the things on which he focused in his farewell address was how dramatically crime changed during his 27 years as a special agent. The criminals he first encountered used knives and wrenches to commit crimes that affected one or two people. Today, however, technically sophisticated criminals using keyboards can have a devastating effect on a hundred or more people.

Gerry's career epitomized those changes. Using sheer determination and extraordinary stamina, Gerry single-handedly pursued case loads that numbered 30 or more early in his career. By the time that career came to a close, Gerry was assigned as the NCIS representative to the Department of Defense Inspector General's Office, where he quickly earned the reputation of being a team player while working on policy affecting the entire Defense Criminal Investigative Organization (DCIO) community.

Gerry's description of a keyboard as a weapon is not an exaggeration. Just look at the article on page 2 about the Computer Investigations and Operations (CIO) Department's efforts to counter the problems posed by the rapid evolution of information technology. It not only takes a lot of people and resources to accomplish the CIO mission, it also takes a lot of training and a willingness to take a "joint approach" to investigations that will allow us to benefit from the knowledge and experience of other agencies. .

There was a time in this organization a number of years ago when some supervisors were not all that enthusiastic about the idea of working with some of their counterparts in other agencies. I wonder what they would think about the article on page 12 recounting the historic events leading up to NCIS signing a memorandum of understanding with the Russian Federal Security Service, known as the FSB. The signing ceremony was held at FSB Headquarters, which just happens to be located on Dzerzhinsky Square in Moscow – in the same building which once housed the headquarters of the KGB.

The days of "going it alone" are over -- if they ever really existed at all. That is why we are putting so much effort into strengthening our bonds within the DCIO community. That is why we must continue to work closely with other federal, state and local law enforcement agencies, and especially with our other military law enforcement partners.

In the same way that the military adjusts to changes in technology, NCIS must be flexible in addressing new criminal threats. As we shift assets to combat computer and economic-related crimes, we must forge closer links with the Marine Corps law enforcement and Navy security communities to ensure seamless law enforcement. I strongly believe that these changes offer us the opportunity to grow and become more valuable to the Department of the Navy as we prepare to fight criminals of the future.

Finally, I would like to take this opportunity to thank all of you for making 1998 an outstanding and productive year, and I wish you and your families Happy Holidays and a Happy New Year.

DAVID L. BRANT

There is a need for enhancing communication between Headquarters and the field elements of the Naval Criminal Investigative Service (NCIS). We can satisfy this need and increase our effectiveness in serving the Department of the Navy by selectively publishing information of interest to the members of NCIS. This Bulletin is intended for use by all members of NCIS.

Rapid Evolution Of Information Technology Poses New Problems In Law Enforcement And Security

By Special Agent L. Lanark Lockard
Computer Investigations and Operations Department

The rapid evolution of information technology (IT) and America embracing of this technology have created a revolution in business, government and military affairs.

Foremost in this revolution is the premise that organizations that effectively share information will out-produce those which do not effectively share information. "Information is power, but only when appropriately shared."

This sharing of information is a cultural change which has been embraced fully by the political and military leadership. It has been equally embraced and utilized by the public.

Whether we approve or disapprove of this revolution is not relevant. It has happened and is continuing to evolve.

We must be able to adapt our traditional means of conducting criminal and counterintelligence operations and investigations to detect our adversary's illicit or dubious activities. They are surely taking advantage of this new, inexpensive technology.

If we do not develop a robust capability to detect, physically apprehend or expose, and prosecute individuals and organizations who use this technology to more efficiently conduct their dubious trade, then we will lose mission, respect and relevance in the near future.

This is not just a network security problem that can be fixed by hardware and software configuration. It is a human, law enforcement, and counterintelligence problem.

OPEN SOURCE

The recent postings of massive quantities of information to on-line sites have made it very easy for foreign intelligence services to cheaply and quickly identify systems and people to target.

What used to require having an operative on site and many days or weeks of collection and analysis can now be done from any location in the world and in a matter of minutes.

This inexpensive means of collection has given any third-rate dictator enormous intelligence capabilities that he or she previously could not afford or found unavailable.

The volume of material available through military Web sites is staggering.

INVESTIGATION AND ANALYSIS

Hackers are persons who use computers and communications systems to gain unauthorized access to computer systems for numerous and varied reasons.

These reasons can range from the entertainment value and the challenge a hacker receives from being able to get into a system to motives of illicit financial gain, vengeance, vandalism, larceny, and espionage.

Much like the solving of a puzzle, some hackers get self-satisfaction and a sense of accomplishment from breaking into a computer and intend no ill to the host computer system or data.

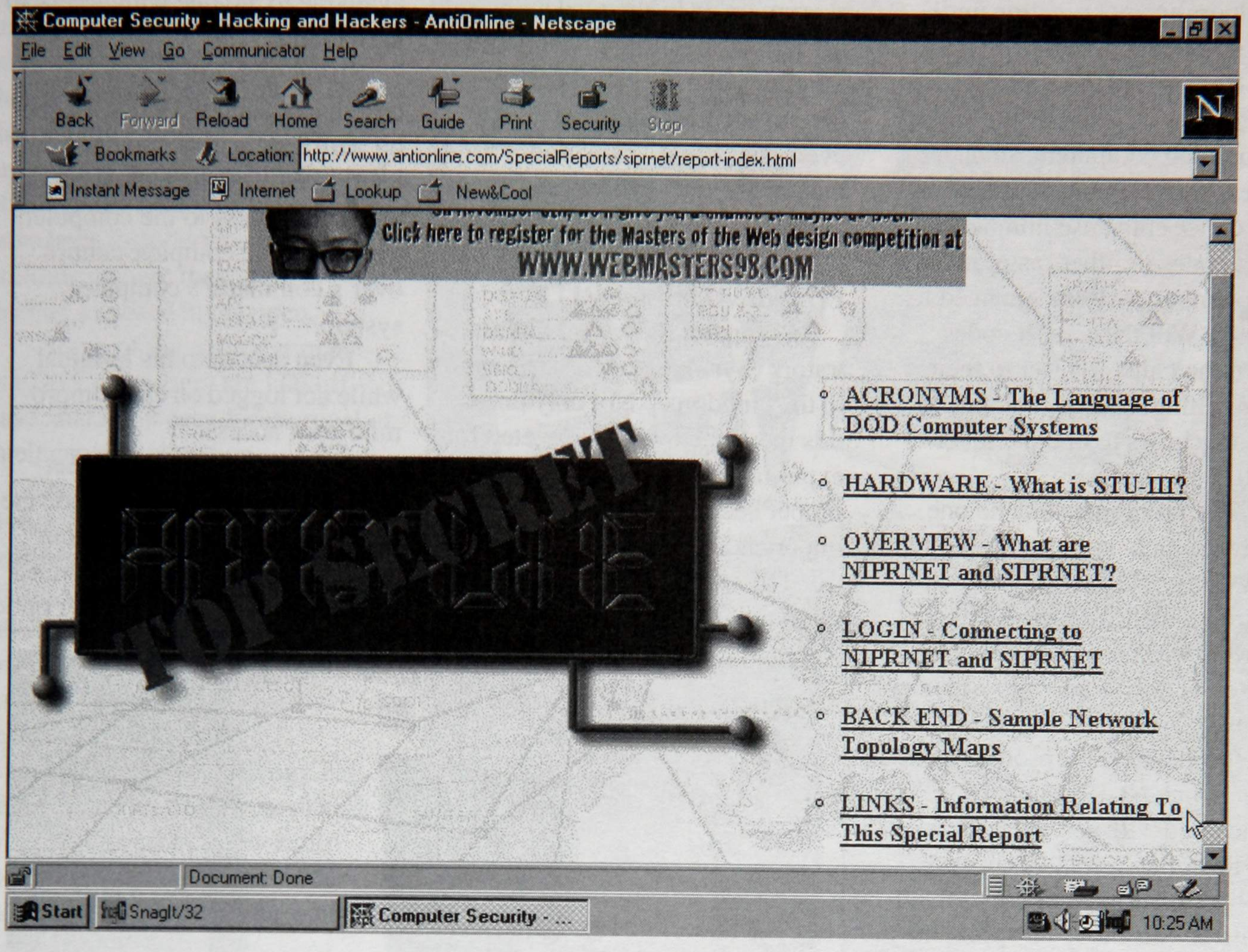
Some will intentionally leave evidence of their intrusion. This type of hacker, like most individuals, likes to brag about his success. He inadvertently advertises vulnerabilities and leaves road maps for others who have more sinister motives. Others are motivated by personal, political, financial or military/paramilitary gains.

THE INSIDER

While hackers appear to be gaining the most attention and publicity, the biggest risk to the security, integrity, availability, and non-repudiation of information on networks are the persons who are authorized users of the network... "The insider".

The lack of security precautions utilized by some users can subject computer networks to intrusions.

Authorized users and systems administrators may intentionally



This is just one of several "hackers" homepages available on the world wide web.

or unintentionally disable security settings of software to accomplish their job, making the system vulnerable to exploitation by criminals and intelligence officers. In a more traditional scenario, an intelligence officer or criminal could co-opt an authorized user to disable security settings or copy sensitive information.

The motives for such actions are tried and true: disgruntled employees; financial gain; ideology/political motivation; blackmail; and others. Numerous examples already exist to show that the infrastructure has been exploited by insiders to commit espionage.

The most recent case is the Robert C. Kim investigation, which was a very simple exploitation of the system. As a matter of fact, the last five espionage cases involved use of the U.S. Government's computer infrastructure.

What will happen when the insider is more adept at copying and transporting sensitive information? Will we have the personnel with an understanding of how this technology will be used by our adversaries?

THE Y2K PROBLEM

The Year 2000 (Y2K) problem is an unknown quantity and real threat to the Department of Defense (DoD), Department of the Navy (DoN), and general public.

Many electronic devices, from electric coffee pots, elevators and burglar alarm systems to medical equipment, personal computers and super computers, are manufactured with electronic chips (parts) which have instructions embedded on them.

Many of these instructions treat dates with the year designated by two digits (98 or 99). By the year 2000, many of the chips will read the year as 1900.

No one is sure how the machines will react when the wrong date is interpreted by the chip. Will the machines dependent upon the chips cease to function because the chip interprets that required maintenance is 100 years overdue?

For example, if maintenance has not been conducted on elevators, they are programmed to stop at the bottom (ground) level, open

the doors and not function until service is conducted.

Now image this with security alarms, banking and financial accounting computers, all data bases, and weapons systems.

Other chips use numbers as reset codes or other instructions (September 9, 1999 changed to 9999). Will these reset codes force the chips to reset to their base setting, causing computers and machines to operate incorrectly?

The problem is that no one knows which systems used by the Navy have chips with these instructions embedded into them or what the instructions are on these ROM (Read Only Memory) chips.

While the Y2K problem is not one which NCIS should be concerned with solving (it is an engineering/systems security problem), the vulnerabilities that could be caused by this problem may be vast and cause an increased work load across the spectrum of NCIS mission areas.

NCIS special agents, particularly those in the Computer Investigations and Operations (CIO) Department, will have to understand the Y2K problems and vulnerabilities when conducting investigations. They will have to be able to distinguish between problems caused by malicious codes installed by a hacker or insider and Y2K problems.

FOREIGN EXPLOITATION

In a situation similar to the Y2K problem, many chips and circuits used in computers, communications equipment, and weapons systems are manufactured in overseas locations.

Likewise, elements of software packages, such as the encryption code included with Microsoft operating systems and programs like the Firewall 1 system security, are written overseas. What "back doors" and malicious codes were programmed into products?

PHYSICAL SECURITY

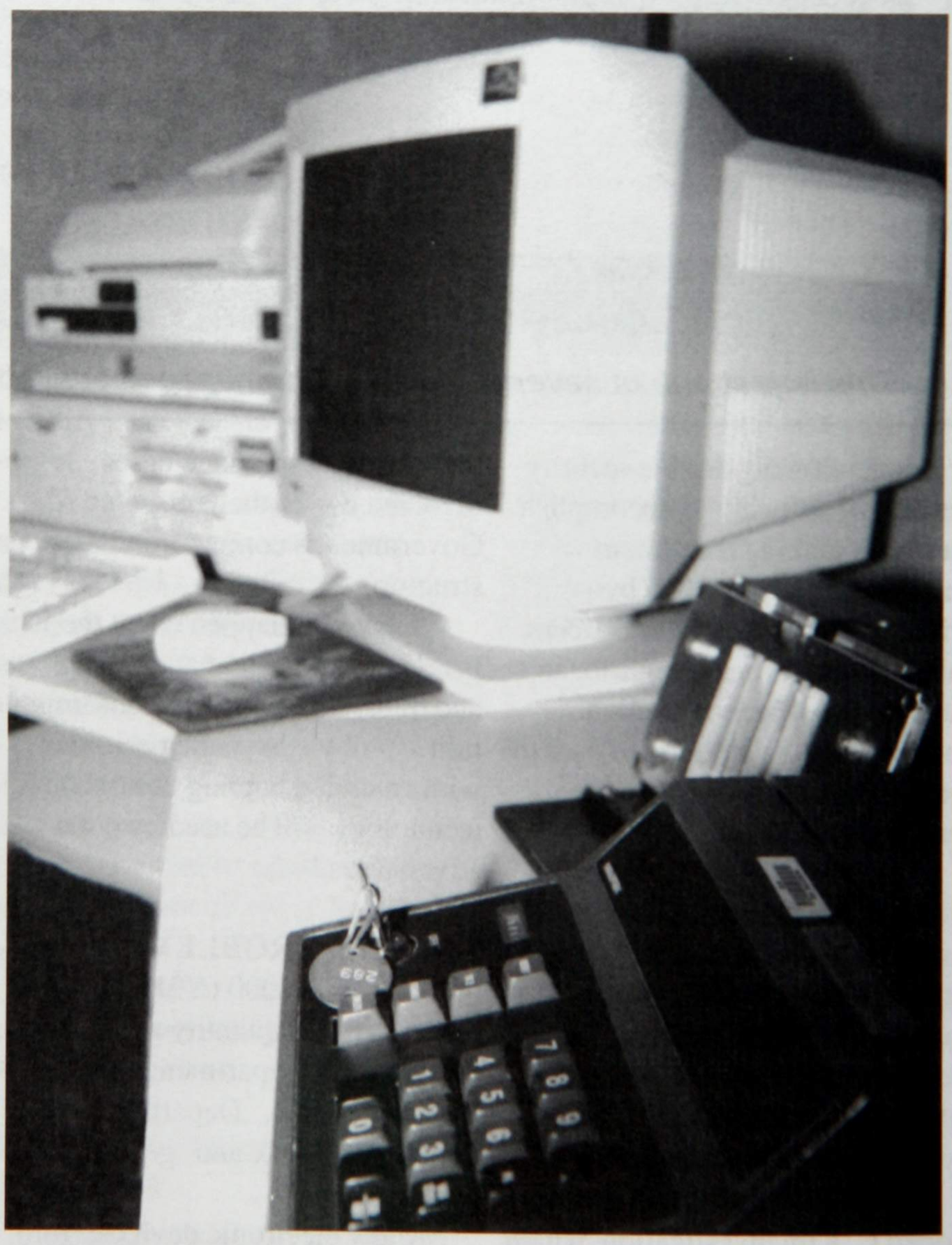
Computer Systems Administrators (Sys Ads) have "the keys to the kingdom." Not only does this mean they will be targeted for exploitation, but their awareness of proper security precautions are important.

The spaces in which they work are frequently unsecured, available to anyone with access to the building.

If the Sys Ad leaves his terminal unattended while logged on with root access, anyone who happened by could set himself up with root access to the computer, giving himself complete control over a command's computer system.

Even access to his terminal while not logged on can compromise root access.

The physical computer network is also vulnerable outside the office and buildings. Computer networks are normally connected by cables. Whether it is fiber optic



Unattended *systems administration stations are an open invitation to tampering.*

or twisted pair (two types of cables used to connect computer and telecommunications systems), they are vulnerable to being cut, thereby disrupting the service, or tapped into in order to monitor and obtain data. Many of these cables have been installed in older buildings where they are frequently exposed in the open.

Some of the cables connecting DoN computers are laid off-base, making it easy for criminal or intelligence exploitation.

On a more sophisticated level, dedicated criminals as well as hostile intelligence services have access to a wide range of highly advanced intercept equipment previously limited to only law enforcement and well-funded security agencies.

The cost of technology has dropped so much that poor, Third World countries can now equip themselves with effective information systems monitoring equipment.

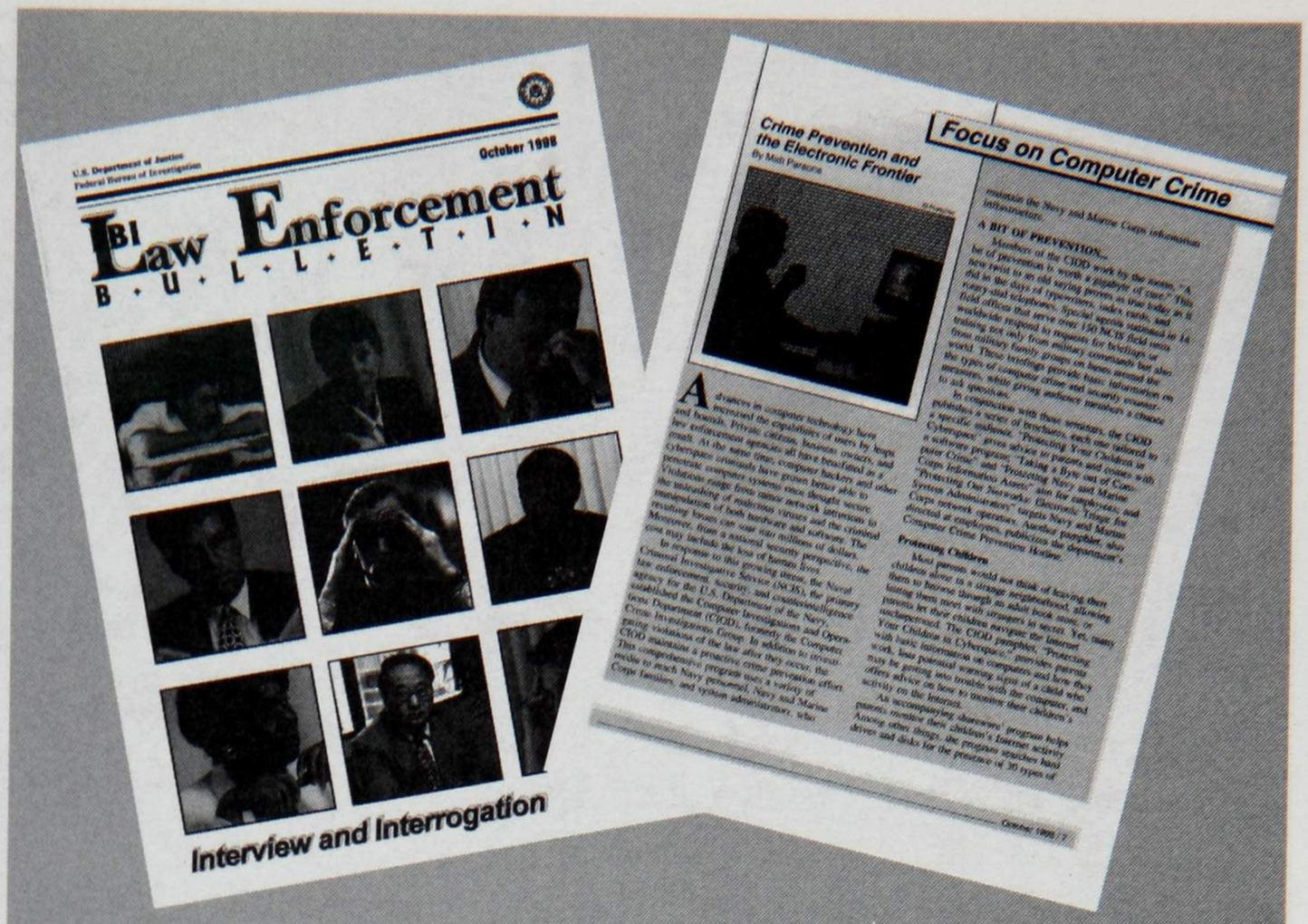
By exploiting physical vulnerabilities, these criminals can observe everything transmitted across the network.

This type of illicit activity is not limited to computer networks. Street criminal elements using store-bought intercept equipment and a laptop computer have captured cell phone identification signals so they can produce clone cell phones.

Technology is expanding so rapidly, in fact, that a host of other new, but unknown technical methods will be arriving on the scene for the foreseeable future.

These threats and the vulnerabilities they pose must be identified as quickly as possible so countermeasures can be taken.

A good example is the rapid development and availability of



NCIS Computer Crimes Articles Appear In The FBI Law Enforcement Bulletin

Two articles about the NCIS Computer Investigations and Operations (CIO) program appeared in the October 1998 edition of the *FBI Law Enforcement Bulletin*.

An article written by Special Agent Matt Parsons entitled "Crime Prevention and the Electronic Frontier" begins on page 7. Another article entitled "The NCIS Computer Intrusion Investigation" is on page 9.

The articles are available on the internet and may be found on the FBI Web Site at "www.fbi.gov" and the NCIS Web Site at "www.ncis.navy.mil."

Hacker's Guide Available On The Infoweb

Special Agent Paul Bright has authored an in-depth, instructional series entitled "Guide to (Mostly) Harmless Hacking," which is available on the CIO Homepage on the internal NCIS "Infoweb."

The series, which is geared to agents who are interested in learning more about this area of information technology, is divided into six volumes.

The highly informative, easy-to-read series covers forging e-mail, fighting spammers, nuking offensive web sites, Linux, port surfing, protecting yourself from e-mail bombs, information warfare, shell programming and advanced hacking techniques.

It is available only to NCIS employees who have access to the internal "Infoweb."

Intrusion Response

Here Is What To Do If You Get "Hacked"

If you have reason to believe that your network has been the subject of an intrusion and your command's sensitive data is being compromised, your first priority should be the protection of the information.

Depending on the sensitivity of the information subject to compromise, you may want to disconnect the system from the internet. Then immediately notify the Navy Computer Incident Response Team (NAVCIRT), the NCIS Intrusion Response Group (IRG), NCIS Computer Investigations and Operations Department (CIO), or the nearest NCIS office.

Here are some important points of contact in the event of an intrusion:

E-mail: navcirt@fiwic.navy.mil
NAVCIRT Toll Free Hotline: 1 (800) 628-8893
NCIS IRG: (757) 464-8036
NCIS CIO: (202) 433-9293
DoN Computer Crime Hotline: 1 (800) 278-9917

The NCIS IRG is co-located with NAVCIRT in the Fleet Information Warfare Center (FIWC) in Norfolk, Virginia, and provides real-time incident evaluation of intrusions for law enforcement or counterintelligence issues.

NCIS recommends the following for system administrators to assist in intrusion investigations:

* Ensure authorized DoN warning banners are in place on your network.
* Backup audit logs on a regular basis.
* After a suspected intrusion, keep separate copies of applicable audit logs for future investigation.
* Do not attempt to "hack back."
* Be prepared to follow the instructions of NAVCIRT and NCIS if an incident occurs.

The above is a short list of recommended actions. For more complete information and instructions, please contact NAVCIRT or NCIS.

The best response to computer intrusions is knowing what to do before they happen.

encryption programs. This is a challenge not only for investigations, but also a legal challenge currently being debated at the highest levels of government.

COMPUTER FRAUD

The "paper-less environment" has ushered in a new phase in fraud investigations. By the year 2000, contractors will be submitting bids electronically, verifying work electronically and being paid electronically.

These are all areas where fraud has traditionally occurred. Bid-rigging, false statements, and theft that previously occurred in paper environments will now be occurring in an electronic environment with no "paper trail" to follow.

Economic espionage is easier with this new information technology. Trade secrets can be obtained through hacking, social engineering and betrayal by disgruntled employees.

Cash transactions via electronic means were once regarded as among the most secure methods of moving money. However, theft of liquid assets is becoming more and more common.

Recently in California, an oil company manipulated the ROM on chips in gas pumps to take advantage of state certification procedures which measured the accuracy of the pumps by measuring the output at 5 and 10 gallons.

The chips' program was changed to pump accurately at 5 and 10 gallons only, and to pump less than indicated at all other amounts.

It is estimated that California consumers were cheated out of millions of dollars.

Will the Navy be a victim of a similar fraud where computers

The CIO Department *met recently to find out what computer talent could be drawn from the NCIS Naval Reserve units. From left to right are: Special Agent Paul Bright; Lt.Cmdr. Kathy Blickle, Reserve Program Coordinator; Special Agent Bob Rauss; Special Agent Lanark Lockard; Deputy Assistant Director Al Zane; and Computer Specialist Mark Bodkin. They are meeting in the new CIO Contingency Center on the third floor at NCIS Headquarters.*

measure or record the quantity or value of a product purchased?

Can money be stolen from your bank account without your knowledge? All of your cash is stored electronically in banks. In reality, the only cash that really exists is that in your pocket!

The remainder of your money is stored in an electronic format. You can withdraw cash from your bank account by use of an access card, such as an ATM or debit card.

For example, purchases at retail stores can be paid through the use of ATM and debit cards.

Can an unscrupulous employee modify the input device to capture your card data and PIN number and later withdraw money from you account?

A few years ago, there were reports of fraudulent ATM machines which provided cash when you accessed your account through the machine; however, the machine captured your access card data and PIN number.

This data was later used to recoup the cash you obtained from the false ATM machine and steal additional cash from your account.

PROLIFERATION OF PERSONAL COMPUTERS

As personal computers become more commonplace in the home, criminals will utilize their capabilities more and more in planning and communicating during conspiracies and, in some cases, the actual commission of crimes.

Just about any crime can be planned using a computer. In fact, one of the more notable cases investigated by NCIS involved the disappearance and murder of a female Marine captain from the Marine Corps Base at Quantico. This case was solved after the suspect's computer and diskette were examined and critical evidence found regarding his plans.

For stalkers, child pornographers, and terrorists, the internet has become a gold mine, providing addresses, telephone numbers and street maps showing the location of residences of their potential victims.

Computer records can also yield "evidence of intent" through correspondence, diaries and other records. This evidence can often mean the difference between conviction and acquittal.

NCIS' CHALLENGE

To meet these and other similar challenges, the NCIS Computer Crimes and Investigations Department was formed in December 1997.

Initially staffed with just a few special agents and technicians, the CIO – also known as Code 20 — has now grown to 31, with plans to expand in response to this type of investigation.

Its purpose is to add a new, and previously unavailable, dimension to the traditional NCIS mission specialties – general criminal investigations, counterintelligence, procurement fraud investigations, and naval security.

To accomplish this, the CIO will need agents from each of the specialties to bring their talent and experience to this new program. In turn, the experience they bring will be vested in support of the programs from which they came.

These agents will acquire new knowledge pertaining to Information Assurance (IA) and Infra-

structure Protection (IP).

They will develop a capability to conduct proactive investigations and operations involving IA and IP. Also, they will work with other similar agencies and units in the DoD and DoN communities, as well as with other federal law enforcement agencies, the intelligence community, and foreign security agencies.

The CIO is currently in the process of establishing an Operations Analysis Center (OAC). This all-source fusion analysis center will support NCIS Investigations and Operations; identify foreign intelligence, terrorist, and criminal activities targeting Navy Information and Technologies residing on IT systems; and assist in developing investigative methods and proactive operations to neutralize identified individuals or groups.

TRAINING

In order to develop and maintain the skills necessary to accomplish the CIO mission, agents must be highly trained. Sources for this training will include courses at the newly-formed Department of Defense Computer Investigation Training Program (DCITP), near the Baltimore-Washington International Airport; the Federal Law Enforcement Training Center in Glynco, Georgia; and through commercial technical education programs.

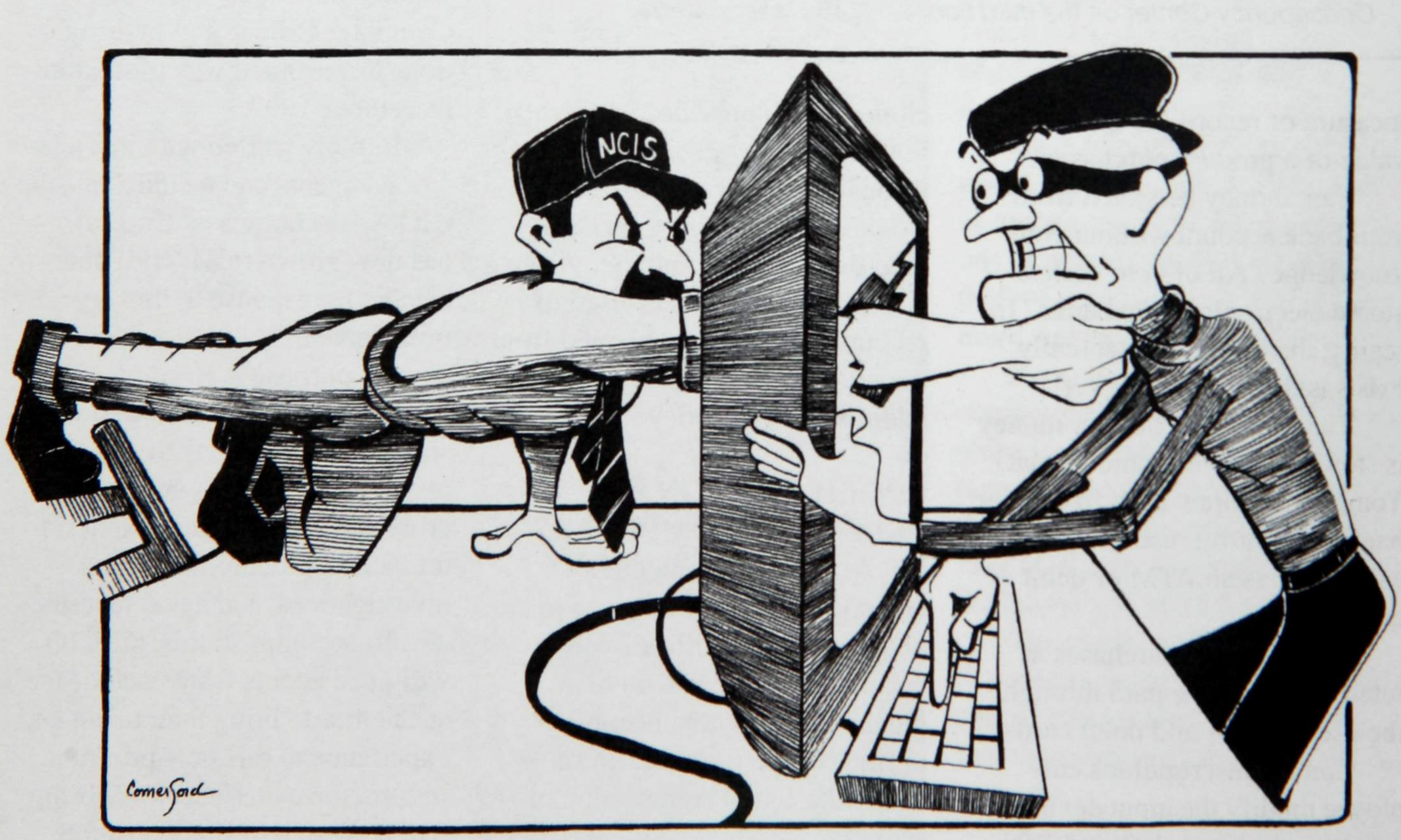
Training will cover the laws of search and seizure in an electronic environment, forensic examination of electronic and magnetic media; internet intrusions investigations; fraud investigations; and counterintelligence investigations and operations in automated environments.

CONCLUSION

The widespread use of automobiles in the early part of this century added a whole new dimension to crime. Law enforcement's response was the radio patrol car.

Today, computers have added a much more dynamic and diverse element to crime which will require a major adjustment in the way law enforcement does business.

The establishment of the NCIS CIO is not the end product. It is the first step in countering a whole new age of crime.



NCIS CIO . . . Fighting Computer Crime!

Commonly Used Computer Terminology

The following list was put together by Special Agent Matt Parsons of the Computer Investigations and Operations Department and includes commonly used computer terms.

Allocation Unit - Smallest area of storage, also known as a cluster.

Analog Computer - A computer that processes continuous data.

Applications - Term used to identify computer programs.

Archive - Attribute that indicates a file has been modified since the last back up.

Attribute - A marker used by DOS to classify or categorize files.

ASCII - Acronym for American Standard Code for Information Interchange. When using DOS, ASCII is often used to refer to a plain text file, which can be viewed, by use of the TYPE command.

Attack - Attempts to bypass security controls on a system. (Active alters data; Passive releases data)

Auto-Answer - Mode of operation that allows a modem to automatically answer an incoming telephone call.

Auto Dial - Feature that enables a computer's modem to dial a telephone number and make connection by itself Sometimes referred to as "War Dialing."

Autoexec.bat - A batch file that is run automatically when you start your computer.

Back up - Method to duplicate files to another device.

Batch File - A text file containing one or more DOS commands; when run, DOS executes each command in turn.

BAUD - Acronym for Bits per second, refers to modem speed. The rate is the measure of speed at which characters are transmitted via modem.

BBS - Bulletin Board System. Software which allows the operator, or System operator, to turn his computer into a public forum. After logging on to the BBS, the user can send and receive electronic mail, read news items, or download files they find of interest.

Bernoulli Drive - External medium for high capacity storage device.

Binary - A counting system that has only two numbers, one and zero.

BIOS - Acronym for Basic Input/Output system. Bios is low-level instructions for the computer providing basic control of the keyboard, disk drives, etc.

BIT - Acronym for Binary Digit. Refers to a single switch inside the computer, which contains the value of one or zero.

Boot - To start up a computer system.

Buffer - An area of memory used for temporary storage of data.

Byte - Amount of space needed to store one character of information.

- Kilobyte - (KB) one thousand bites.
- Megabyte - (MB) one million bytes. (A typical 240mb hard drive could hold up to 27 four-drawer filing cabinets of information.
- Gigabyte - (GB) one billion bytes.
- Terrabyte - (WOW) one million megabytes.

Cache - An area of memory used to hold data recently read from the hard drive.

Capacity - The total number of bytes that can be stored in memory.

CD-ROM - Acronym for Compact Disk - Read Only Memory.

Clipboard - An area of memory that holds text, graphics or other information cut or copied from an application.

CMOS - Refers to special memory inside the computer which stores data about the PC's configuration, hard drive, date and time. Maintained by battery.

Command.com - A file that is automatically run when the computer is booted, contains internal DOS commands, error messages, etc.

Computer - An electronic device that can perform computations, including arithmetic and logical operations; also is capable of storing data.

Computer program - A series of instructions which directs the computer to perform a sequence of tasks that produce a desired output.

Conventional Memory - The first 640 Kbytes of memory on any computer that uses the 80286, 8086, or 80486 microprocessor.

CPU - Acronym for Central Processing Unit. Another name for the computer's microprocessor.

Cracking - The act of breaking into a computer system; what a (cracker) does. Contrary to widespread myth, this does not usually involve some mysterious leap of hackerly brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. Accordingly, most crackers are only mediocre hackers.

Crack Root - To defeat the security system of a UNIX machine and gain (root) privileges thereby; see (cracking).

Data - What you create and manipulate when you use a computer.

Device Drivers - A program that allows the operating system to use a physical device or adds some capability to DOS or windows. Device drivers are installed by a means of commands in CONFIG.SYS.

Directory - A collection of files within a specified storage area.

Disk Drive - Physical location of disks on a computer. Generally, internal hard drives are usually labeled as C Drive. Floppy drives are generally identified as A Drive or B Drive.

Domain Name Services (DNS) - Translates IP address to a "friendly" name such as "ncis.navy.mil".

DOS - Disk Operating System.

Down Load - To transfer data, files, pictures from one computer to another.

Electronic Mail (E-Mail) -Provides for the transmission of messages and files between computers over a communications network.

Encryption - Coding of data for storage or transmission.

Expansion Card - Hardware that attaches to the PC to expand the capabilities of the PC

File - A collection of information is stored as a file.

File Server - A computer on a network that stores the programs and data files shared by the users of the network. A file server is the nerve center of the network, and also acts as a remote disk drive, enabling users to store information. It can be physically located in a different judicial district from the suspect's computer.

Finger – Finds information on users. (name, terminal, access, time of login, phone)

Floppy Disk - magnetic media capable of storing large amounts of information. For example, a 5 1/4" disk can hold as much as 240 sheets of paper; a 3 1/2" disk can hold as much as 470 sheets of paper.

Format - Process of preparing a hard drive or diskette for use by DOS.

Fragmentation - Condition where the file is not stored in contiguous clusters.

FTP - File transfer protocol (download)

GIGO - Acronym for Garbage in - Garbage out.

Graphic File Format - file name extensions used to identify graphic files. The extensions can include: GIF, TIF, PCX, BMP, GL, AVI, DL, FLI, and others.

Grep - Search for text in file(s)

Racker - Not necessarily a negative term. A person who learns about computers by trial and error.

Hard Disk - a means of data storage generally located inside a computer, and not removable. The amount of storage varies from 40mb to more than 1 .2gigabytes in newer systems. As the technology develops, storage size will also continue to grow.

Hidden Files - File attribute assigned by the operating system. Not normally displayed with a standard directory command.

Internet Protocol (IP) Addresses - Address of system on the Internet with standard format across platforms. For example, the IP address of the NCIS Homepage is "138.147.50.102". If you are unable to access the NCIS Homepage from your office computer when you type in "ncis.navy.mil" in the address line, it is most likely caused by a firewall conflict. Instead, try entering just the IP address and you should be able to get it.

IRC - Internet Relay Chat (Public forum to exchange information on Net.)

Macro - A program written within a program, usually designed to carry out some complex operations, automate a series of commands.

Microsecond - One millionth of a second.

Modem - Acronym for Modulator-Demodulator. Converts a computer's digital impulses into a series of analog beeps that are sent over a telephone line.

Motherboard - The main circuit board inside the computer. Contains the microprocessor, some memory and expansion slots.

Multitasking - Simultaneous processing of two or more applications.

Memory Resident Program - A program that remains in memory after it is no longer running.

Network - Grouping of computers to share programs, files through the use of a file server.

NID - Acronym for Network Intrusion Detection.

Operating systems - UNIX, Windows 3.1, 95/98 NT, DOS, Banyan Vines, MacIntosh, LINUX, others

Parallel Port - Connection on the back of the PC usually used for the printer.

Parity - A method of error checking sometimes used with printers connected to a serial port and with communications via modem. There are four types: odd, even, mark and space.

Phreak(er) - One who "hacks" the telephone system to obtain free long distance calling, among other things.

PIF - Acronym for Program Information File. Provides Microsoft windows the details on how to run non-windows applications.

Piracy - The copying and use of computer programs in violation of copyright and trade secret laws.

Port – Connection on the back of the computer to which various peripherals are attached.

Program – A series of commands that instructs a computer to perform a desired task.

RAM - Acronym for Random Access Memory. Primary type of memory storage in a PC. It may also be referred to as Electronic Memory.

rlogin - Logs into a remote system

ROM - Acronym for Read only Memory. Currently, CD-ROM disks generally available in read only format. In the future, however, CD's will be able to be written to, as a floppy disk is now.

Root Directory - Primary directory on every DOS disk.

Scanner - A device which can look at a typed page or a photograph, convert it to digital format, and copy it onto a disk.

SCSI - Pronounced "Scuzzy" refers to a configuration used to connect a device to a computer.

Serial Port - Connection on back of the computer. Usually used for a modem.

Shareware - Type of software available on BBS's which is generally free to try. If users find the program useful, they are expected to send a nominal fee to the author.

"Sniffer" - Program which monitors all information sent over a local area network (LAN) and silently capture 20, 50 or 128 characters sent over each network connection.

Social Engineering - Use of lies, deceit, etc., to convince a legitimate user to divulge system secrets or passwords.

Software - Another term for applications or programs.

Spoof – A trick that causes an authorized user to perform an action that violates system security or that gives away information.

Subdirectory - Term for a directory in relation to another directory. All directories on a disk are subdirectories of the root directory.

Swap file - A file in windows that is used to store information temporarily on disk when memory becomes flill.

System Administrator - referred to as the "sys op" or "sys ad". The individual responsible for assuring that the computer network is functioning properly and for system security.

Tar - Archives files in Unix

Telnet - log in to a remote system.

Trap Door - Hidden mechanism to allow normal system protection to be circumvented.

Trashing - To scavenge through a business' garbage looking for useful information.

Trojan Horse - Appears to perform a useful function but hides an unauthorized program inside.

TSR - Acronym for a Terminate but Stay Resident program.

Virtual Memory - Use of permanent storage medium, such as a hard disk, as though it were memory.

Virus - A code fragment that reproduces by attaching to another program. Damages data directly or degrades/shuts down the system.

Who - Displays names and other information about users on the system.

Worm - Independent program that reproduces by copying itself from one system to another. May damage data directly or degrade/shutdown the system.

Sources: Various sources including FLETC and gcneral criminal tenninology

This building was the headquarters of the former KGB and housed Lubianka Prison.

"Timeshare" Leads To Cooperation Pact Between Two Former Cold War Foes

By Special Agent Thomas Hadaway
Counterintelligence Directorate

It wasn't that many years ago that it would have been unthinkable for NCIS special agents to visit, much less be welcome in the building that housed KGB Headquarters in Moscow. But in a history-making event just a few months ago, that is exactly what happened.

Assistant Director for Counterintelligence Joseph J. Hefferon, Special Agent Bernye Ayer of the Hawaii Field Office and several other NCIS special agents were in the Russian capital in July to execute the first ever bilateral exchange between a U.S. military law enforcement agency and the Russian Federal Security Service (FSB), formerly known as the KGB.

The signing of the agreement was the culmination of a project initiated by the Hawaii Field Office under Special Agent Ayer's leadership and developed under the direction of Assistant Director Hefferon.

The project, which was called *Timeshare*, was developed in direct support of U.S. national security strategy, national military strategy, and USCINCPAC's regional strategy of shaping, responding, and planning now through Cooperative Engagement with the Russian Federation at all levels to support U.S. interests.

Cooperative engagement is defined as 'a future shaping strategy or a process that seeks to promote a sense of partnership.' It facilitates greater participation and increased security sharing responsibility by friends and allies in security matters of mutual concern.

This initiative also required extraordinary coordination between the NCIS, CINCPACFLT, U.S. Defense Attaché's Office (USDAO) Moscow, the Joint Staff, the Federal Bureau of Investigation and the Central Intelligence Agency. Operating in direct support of the Joint Staff (J5) and Pacific Fleet

operations, this project was formally approved for execution in 1997.

In July 1997, the first bilateral conference was conducted between the NCIS and Russian FSB in Hawaii. The primary objective of the initial evolution was to develop standard protocol and operating procedures for providing force protection support to our respective services in the Pacific region. Both parties agreed in principle to prescribed coordination and communications procedures; information and personnel exchanges; and efforts to conduct cooperative actions in support of scheduled event(s) such as port visits, exercises, etc.

During June and July 1998, the second conference between NCIS and the Russian FSB was conducted in Moscow. This meeting resulted in the signing of the first Memorandum of Understanding (MOU) between a foreign law enforcement agency and a U.S. military law enforcement agency. Assistant Director Joseph Hefferon and FSB Deputy Director Oleg M. Osobenkov established this precedent with the signing of the MOU on July 1, 1998.

The MOU formalized the bilateral relationship between FSB and the NCIS. It developed standard protocol and operating procedures for providing force protection support to each participant's respective navies and marines worldwide.

Both parties exchanged the texts of laws and other regulations with regard to providing law enforcement and force protection matters.

The parties agreed that all cooperation and mutual support would be conducted in accordance with these laws and regulations.

According to the protocols established by the

Representatives of NCIS *and the FSB discuss final details during a meeting held in the office of the late Yuri Andropov, who was head of the KGB and later General Secretary of the Soviet Union.*

Below, Assistant Director Joseph Hefferon and FSB Deputy Director Oleg M. Osobenkov sign copies of the memorandum of understanding during a ceremony held in FSB Headquarters on Dzerzhinsky Square.

MOU, all routine communications between the FSB and the NCIS shall be conducted through the United States Defense Attaché's Office (USDAO) at the American Embassy in Moscow.

Following coordination with the USDAO, direct communications between field level operational units of the respective services shall be authorized. The FSB and NCIS will identify points of contact and communications procedures to facilitate this direct line of communications.

The protocols also stipulate that information shall be exchanged prior to scheduled events. This exchange may occur through the USDAO and/or direct liaison between personnel of the FSB and NCIS.

The information exchange will involve written and/ or verbal threat assessments, port surveys, or other information relevant to a specific area or event. All parties will cooperate, render mutual assistance, and exchange information on the following:

Background
- Local government, police, and security structures
- Local customs
- Established procedures/limitations for the handling of incidents

Internal Security Threat
- Local dissident or anti-government organizations and activities
- Terrorism-related matters

General Criminal Threat
- Violent crime
- Organized crime
- Street Crime (e.g., theft)
- Vice Activity (e.g., narcotics, gambling, prostitution, smuggling)
- Racial/Hate Groups

Off- Limit Areas
- Criminal
- Security and medical
- Local hospitals and procedures
- Local medical concerns

Points of Contact
- Identify Headquarters and field level (includes afloat units) points of contact and contact procedures

Special Agent in Charge Bernye Ayer *and Assistant Director Hefferon, flanked by FSB counterparts, pose for a picture in back of Yuri Andropov's desk.*

In addition to the exchange of information, the FSB and NCIS will plan and execute cooperative actions in support of a scheduled event.

For the purpose of the MOU, cooperative actions refers to cooperation in criminal investigations, narcotics suppression operations, security escort details, and the exchange of advance parties to facilitate liaison and coordination in support of the scheduled event.

The FSB and NCIS will exchange delegations on an annual basis and conduct other meetings as required. Considerations will be given exchanging personnel for formal training and to develop a greater understanding of our respective force protection missions.

The MOU will be reviewed periodically by both parties to ensure that the relationship remains mutually beneficial for our respective military services. The agreement remains effective until terminated by either party.

Requests for termination or changes shall be submitted in writing to the respective Director of either the FSB or NCIS. Changes to the MOU will be mutually agreed upon.

Both English and Russian versions of the MOU were signed by Assistant Director Hefferon and Deputy Director Oleg M. Osobenkov of the FSB.

Timeshare is an example of how the NCIS counterintelligence and force protection missions have evolved and are keeping pace with national and theater priorities.

While it was initiated in the Pacific Theater, all parties agree that this initiative has both global and

multi-service implications for the future. *Timeshare* has now transitioned to an NCIS Headquarters-controlled program.

With USCINCPAC sponsorship, NCIS will host the third NCIS-FSB conference in Washington DC in 1999.

In addition to Assistant Director Hefferon and Special Agent in Charge Ayer, the NCIS delegation to Moscow included Special Agents Brian Richards and Bradley Howell. Special Agents Peter Flynn and Virginia Kirk conducted oversight responsibilities of *Timeshare* from NCIS Headquarters Pacific Division. Additionally, *Timeshare* was provided with direct support from Lt.Cmdr. Robert Nugent, Assistant Naval Attaché, Moscow.

Feedback on *Timeshare* has come from all levels of the Department of Defense. The Joint Staff (J5) wrote, "Program received high praise from Secretary of Defense William Cohen, former Secretary of Defense William Perry, Deputy Assistant Secretary for Policy (Russia), Catherine Kelleher, Admiral Joseph Prueher, USCINCPAC, and Brigadier General John Reppert, USDAO Moscow, for being highly innovative and successful."

History In The Making

FSB Deputy Director Osobenkov and Assistant Director Hefferon, above, exchange gifts following the signing ceremony in the old KGB Headquarters.

At left, Assistant Director Hefferon presents a framed NCIS poster to FSB members following lunch in the former KGB compound outside of Moscow.

Special Agent Uses EOD Experience To Draft Ready-Reference For Post-Blast Investigations

By Special Agent Jeffrey H. Norwitz
NCIS Far East Field Office

Author's Note: *This article was written to aid field investigators with investigating bombings and post-blast crime scenes. This material is a ready-reference source when faced with the infrequent, but technically challenging task of investigating explosions of any type.*

Often, when incidents occur involving an explosive device, investigators lack resource material in the field and explosive ordnance disposal (EOD) personnel may not be available. Having a basic understanding of this information enables the investigator to recover evidence, make meaningful observations of the crime scene and arrive at professional conclusions after post-blast examinations.

Increased knowledge also results in better communications with counterparts of other agencies when discussing such events.

Section one provides background information pertaining to the science and physics of explosions. The three major types of explosions are addressed with guidelines concerning unique evidence, which differentiates the three post-blast scenes.

This data enables an investigator to prepare technically accurate reports, incorporating correct terminology, and make investigative conclusions regarding the criminal or noncriminal cause of an explosion.

Section two is a discussion of explosive evidence collection and observations of post-blast scenes. Suggestions of what to look for, what questions to ask, and proven investigative strategies are presented. Review of this material will aid in the processing of crime scenes and the collection of relevant evidence.

A final section is devoted to proper and safe methodology for searching motor vehicles for explosive devices pursuant to an investigation or protective service detail. Should EOD resources not be available, this guide should provide a foundation for an investigator to conduct a safe and thorough examination of the scene.

This article is not designed to be an exhaustive study of the subject matter but, rather, to highlight topics and suggest areas that can be further researched with local sources.

THE SCIENCE OF EXPLOSIONS

An explosion is a rapid combustion, decomposition, or deflagration, which results in a sudden tremendous release of gases and an instantaneous violent increase in pressure, accompanied by a loud noise and high temperature.

There are three basic types of explosions of interest to criminal investigators:

- Flammable gases - natural gas, gasoline, ether, propane
- Pressure vessels - steam boiler, compressed air tank
- Chemical explosives - dynamite, TNT, plastique compositions

FLAMMABLE GAS EXPLOSIONS

Gases are not flammable without the presence of oxygen in definite proportions. The percent of flammable gas by volume must fall within what is known as the "Flammable Limits" or the "Explosive Range".

These limits are the points at which the mixture is too lean or too rich to ignite. The percent of flammable gas in the mixture has a great influence on the violence of the explosion, the pressure developed, and the amount of flame.

Most gas explosions generate pressures of between 20-25 psi but can reach as high as 100-125 psi. Dust explosions are similar to gas explosions in effects and principle and are included here for discussion.

Gas explosions basically affect only the things that tend to confine them (walls, ceilings, roofs, floors) and produce no direct shattering effect. In some instances a gas explosion victim may be blown out of a building without injury.

Gas explosions result in a pushing effect rather than a shattering effect. Exterior walls tend to break in sections and will usually be found lying flat, but almost intact. A gas explosion within a wall will cause one side of the wall to go in one direction, while the other side goes in the opposite direction.

Gas explosions create no cratering effect, nor will any specific point of origin be evident. Caution must be exercised not to mistake concrete "spoiling" for cratering. Spoiling occurs when flaming liquid settles on concrete and causes the moisture in the cement to boil. Small steam explosions shatter the surface of the floor and look like craters.

Furnishings in a room will show no signs of blast damage and often the explosion does not move them as there is equal pressure built up from all sides. They may show signs of intense heat (charring, melting) or be disturbed by secondary projectiles but you will not find furniture thrown great distances from the structure. Collapsing of sealed metal cans, equally on all sides (similar to a squeeze by a giant hand), indicates the explosion of gas vapors.

The theory that bombers have trademarks and construction habits is very true.

The recovery of a device intact is a tremendous asset to case resolution.

Explosions involving natural gas or other lighter-than-air gases will frequently raise the entire roof of a building momentarily. When this occurs, the walls, not having any tie support for the moment, will fall outward, often completely intact. As the roof comes back down, also usually intact, damage to the furnishings results and the occupants become trapped under the roof debris.

An explosion of this type in the basement creates a heaving effect usually raising the entire house off its foundation and damaging interior and exterior walls on the floors above.

Explosions involving gasoline or other heavier-than-air gases will result in the walls of a building being forced outward at the floor or plate level with normally little blast damage higher up on the walls, ceiling or roof area.

Often flash marks will be found on materials between the source of ignition and source of gas. Flash marks are caused when the flammable gas vapors become ignited at the source and travel back to the heaviest concentration of fuel.

Because these vapors are at the lower flammable limits when they reach the source of ignition, the amount of flame and heat is not sufficient to ignite combustible materials and the result is scorching or charring of light combustibles such as paper, plastic or curtains. This scorching will be lightest in the area of the ignition and will become more distinct closer to the source of supply.

The noise associated with a flammable gas explosion produces more of a rumbling effect (similar to thunder) rather than a sharp crack. Witness accounts are invaluable concerning this point.

PRESSURE VESSEL EXPLOSIONS

Cause of the explosion is usually apparent due to the destruction of the appliance involved. There will be heavy damage in the immediate area to buildings and contents from fragmentation of the appliance. Portions of the vessel will frequently be found embedded in plaster walls, wood paneling, ceiling and furnishings.

CHEMICAL EXPLOSIONS

Explosions involving chemical explosives or blasting agents will show a distinct point of detonation, which can be readily identified due to the fact that the greatest amount of damage and destruction occurred at this point.

Usually cratering will be present as well as severe shattering effects. In the case of explosives such as dynamite, residue from the explosive may be apparent in the debris at the blast point. Often, unexploded fragments or portions of the explosive can be found.

Depending upon the detonating velocity (brisance) of the explosive, severe shattering effect may be found for some distance. High velocity explosives such as nitroglycerin and TNT tend to produce almost complete disintegration at the point of

explosion. Low velocity chemical explosions, such as black powder or a homemade compound, will still be evidenced by shattering but far less dramatic.

Debris from a chemical explosion will normally be found at a much greater distance than in the case of a gas explosion. Victims and property are injured/ damaged mainly on the side facing the center of the explosion.

The main destructive effects of chemical explosions are:

· Blast - A wave of compressed air moving out from the point of detonation at approximately 1,100 feet per second (fps) and resulting in pressures of up to one million psi.

· Heat - Temperatures of 3,000 - 4,000 degrees Fahrenheit are not uncommon.

· Fragmentation - Portions of the device and debris moving away from the point of detonation at velocities of approximately 20,000 fps.

· Suction - Air waves return to the point of detonation at speeds nearly equal to the blast wave (1,100 fps).

Thus far, we have discussed the science of explosions and the physical effects of explosive events. For the criminal investigator, the immediate challenge at a post-blast scene is the determination of "probable cause" (i.e. criminal vice accidental) and collection of evidence to support the conclusion.

The remainder of this article addresses basic methodology and theory to help the field investigator reach those objectives.

INVESTIGATING EXPLOSIONS

A criminal bomb is an explosive device which is placed, dropped, thrown or projected with the unlawful intention of causing injury, death, destruction of property, disturbance, coercion or intimidation. Thorough investigation of evidence can develop valuable leads and certainly corroborate or refute informant information.

The examination of the post-blast scene will often enable one to draw reliable conclusions as to the nature of the explosive causing the damage, quantity of explosive, container, initiation and means of delivery. The type of explosive used may lead to the bombers.

***A Greek police officer** looks over the remains of the car bombing in which Navy Capt. William Nordeen was killed in 1989.* (NCIS Photo)

Contrary to popular belief, building a properly functioning bomb that consumes the entire explosive, detonates at the right moment and performs in accordance to design, is not an easy task.

As a result, many cases are solved because the bomber either kills him/herself in the construction or transportation phase. Others are solved because the device fails to function, leaving a treasure of physical evidence.

The theory that bombers have trademarks and construction habits is true. The recovery of a device intact is a tremendous asset to case resolution.

The question is often asked of investigators, "What kind of explosive was used?" The answer may be self-evident if the explosive is not completely consumed. The term for this is "low order". Low order explosions are caused by either defective explosives or inadequate priming. In the case of dynamite, one should be aware that dynamite consists of a mixture of chemicals, some of which are oxidizing salts. These salts are hygroscopic and will draw moisture from the air and ruin the initiation sensitivity of the dynamite.

Improper storage, humid atmosphere, and opening or breaking the cartridges will cause the dynamite to desensitize. A low order dynamite explosion will leave pieces of dynamite in the bottom of the crater or scattered around the area. Composition "C" plastique explosives require a special blasting cap surrounded

at the base by the explosive to insure detonation.

Smaller caps improperly placed will result in misfires and scattering of all or part of the composition explosive, resulting in a low order blast.

Misfires of the blasting cap result in the entire device being found intact. Misfires with fuse caps are usually caused by a faulty crimp of the cap to the fuse. Misfires with electric caps are usually due to faulty contacts or firing connections.

Shunts from electric blasting caps, the color of the wires, and parts of the electric cap will identify the manufacturer. If a small charge is used or if the cap is partially inserted in the explosive, the top part of the cap (plug) will be found.

If an explosion takes place in midair, there will be no central crater but, instead, a radiation or sunburst pattern on objects surrounding the explosion center.

Questioning of witnesses as to the type and distance of the sound and color of the explosion, the amount and color of the smoke and the violence of the concussion (as evidenced by ringing of the ears) may be of value in corroborating the results of physical examination. Black smoke indicates RDX, TNT, or PETN explosive. Black or gray smoke indicates an excess of carbon to oxygen in the explosion. Dynamite and gunpowder give white smoke. Smoke quickly dissipates in open areas but will remain in buildings for some time.

Photographs of post-blast scenes are of particular value. A trained expert can "read" post-blast photographs and provide valuable insight. If possible, obtain photographs of the building, inside and out, taken prior to the blast.

Aerial photos are of great value as they can reveal much about the debris pattern not easily seen from ground level. Make notes of the size and distance which large pieces of debris are thrown. Such notes can be used to evaluate the size of the device.

The center of the explosion should be sniffed and a gas collection tube utilized to collect a sample of gas where odor is strongest.

A sweetish smell may indicate dynamite, while an acrid smell or absence of smell may indicate military explosives. Atmospheric samples near the center of the explosion where the odor is strongest may be collected with vacuum bottles or "grab bottles".

A grab bottle can be improvised by filling a clean soft drink bottle with water and then emptying it where the odor is strongest. The air is capped for gas chromatography analysis.

Discoloration of surfaces near the crater are often black carbon contaminated by pulverized material. White discoloration is often found at composition "C" explosions, although this should not be the only reason for eliminating other explosives.

Samples of the soil from the center of the crater are of great value in determining the identity of the explosive. Remember to obtain a sample from nearby uncontaminated soil for comparison. A clean paint can with a tight-fitting lid is best for soil samples. The air in the can is later tested for explosive residue.

Fuse gives off white smoke when it burns. A line of black soot or tar is left when fuse burns across a surface. In the investigation of an explosion, marks may be found on an adjacent wall where recently burned hot fuse has ricocheted and left tar or fiber wrapping marks and fuse color. Chemical analysis of these marks may confirm that it was fuse.

The best surfaces to collect for chemical analysis are any metal, wood, or cement discolored by the explosion. Metal that rusts within a few hours of a bombing indicates the presence of oxidizing salts as found in dynamite. An appearance of spider web sublimation on the surface of metal at cold temperature indicates dynamite.

The debris should be carefully searched for physical evidence, which may give clues to the type of container. It may also establish the type of electric

A Navy enlisted woman *was killed when a car bomb exploded outside a night club, shown above, in Naples in 1988.* (NCIS Photo)

Two people were killed *and 11 injured when a car bomb exploded at Rhein Main Air Force Base In Germany in 1985.*

(Department of Defense Photos)

current, whether battery or house current. Hand grenade spoons are found en route from the position of the thrower to the target. The evidence may consist of pipe, can or other container, wrapping of cloth, electrician tape, rope, wire, fragments of burned fuse, fragments of blasting caps, batteries, clock works, and so on. Anything which is foreign to the immediate surroundings should be suspect.

A magnet dragged through the crater and immediate area also may collect unseen evidence. The dirt in the center of the crater should be searched to a depth of about two feet. The blast forces bomb parts straight down into the ground which are then covered up by falling dirt from the blast.

An explosion creates a vacuum effect by movement of air pressure. The air pressure moving back to refill the vacuum immediately follows this. This implosion will cause breaking windows and objects to move toward the center of the explosion. Small light debris may be sucked into the crater further, covering the surviving bomb parts.

An improvised sifter can be made from screen remnants or other like material and used to facilitate the search for surviving evidence.

If elongated scratches, gouges or holes are found driven into surrounding objects, there is a strong possibility the explosive material was placed in a container, which was turned into shrapnel by the explosion. Pieces of the bomb are called "primary fragments".

Pieces of objects from the scene are called "secondary fragmentation." Container fragments that are small or sharp with a torn appearance indicate that the explosive filler was a 'high explosive" such as TNT or dynamite.

"Low explosives" such as black powder or homemade substances leave large container fragments with a cracked appearance.

Take notice that a bomb must be placed, dropped or thrown and that somehow the perpetrator transported the device to the target. To do so safely, the bomber must devise a "safe transport" mode for the device to avoid premature detonation. Often that consists of a pull string, safety wire, insulator strip that is removed after placement. These items are usually discarded and found nearby as they survive the blast.

Teaspoon-size fragments of explosive can be analyzed to determine which company manufactured the substance. Each explosive manufacturer has unique formulations, which can easily be identified. In the case of civilian dynamites, some contain small flakes of material called "tagent 5" which are added to the explosive by the manufacturer and which survive the blast. Recovered tagents are examined by microscope and reveal a serial number-like identification that can then be traced.

Evidence obtained in the manner described may be of great value in determining the bomb's origin, and thereby aid in bringing about the arrest of the perpetrator(s).

The source of the material used in the bomb

should be traced to determine the manufacturers, distributors, and users. It may be found that a particular part is rare and the bomber identified as the purchaser.

Finally, experience has shown that, once a bomber finds a device that works, he will build other devices exactly like the successful one. So much so that the same color wire, type of tape, brand of battery, type of watch, etc. will be found in successive devices built by the same person.

In the case of organized terrorist groups, bomb construction is almost like a trademark. Typically, one or two members are designated as the "experts" and they will build clone devices for distribution throughout the group. Often these persons will publish "approved" blueprints for bomb construction, which will also be disseminated.

The novice, who is following the blueprints, will build his device exactly as per directions for fear of killing him/herself. This results in look-alike devices being built by different persons, thousands of miles apart, but identifiable with a particular group because of construction techniques.

Proper evidence collection will memorialize the event like a fingerprint. Other bombings can be compared via evidence examination and make valuable matches, helping identify the responsible.

The Author

Special Agent Jeff Norwitz formerly commanded the bomb squad of the El Paso County Sheriff's Department (EPSD) in Colorado Springs and was a guiding member of the International Association of Bomb Technicians and Investigators.

Norwitz is a 1981 graduate of the Hazardous Devices School in Huntsville, Alabama, and numerous FBI and ATF courses on disposal of explosives and advanced techniques of post-blast investigations.

During his tenure with EPSD, he responded to over 500 bomb-related matters and safely removed or disarmed scores of improvised explosive devices.

Norwitz is currently assigned to the Far East Field Office.

The Explosive Ordance Disposal (EOD) *technician's badge, shown above, is worn by military and some civilian law enforcement personnel. Due to its shape, it is sometimes referred to as the EOD "crab."*

A checklist for searching motorcade vehicles is on the next two pages.

PERSONAL SECURITY DETAIL TECHNIQUES FOR SEARCHING MOTORCADE VEHICLES

The search of vehicles usually includes the principal's limousine, the follow-up and the spare car. Vehicle searches consume about 20 minutes per vehicle for one man, and should be timed to be completed about 30 minutes prior to the principal's arrival. Searches are conducted in areas where the least amount of attention is attracted and should not be done without physical security.

The search of a motor vehicle should be made each time there is a movement of the protectee unless the vehicle has been under constant surveillance by security personnel.

The guidelines given below are based upon the situation where at the beginning of the search there has been neither a threat made nor any other cause for unusual suspicion. Consequently, remote opening procedures are not detailed here and are left to the personal discretion of the search personnel.

BEFORE TOUCHING THE VEHICLE, CONDUCT AN EXTERNAL SEARCH AS FOLLOWS:

- Check the area around the vehicle. Look for bits of tape, wire, string, time fuse, etc., around the target.
- Look for marks on the ground, such as footprints, jack stands impressions, etc.
- Look for signs of forced entry: around doors and windows, at the trunk, on the hood. Fingerprints on the trunk, hood, or wheel covers might indicate recent opening.
- Look inside the vehicle, through the windows, for any obvious devices or packages that may not belong there.

THE MOST LIKELY SPOT TO FIND A BOMB, IF THE VEHICLE IS LOCKED, IS UNDER THE VEHICLE. LOOK UNDER THE VEHICLE FOR THE FOLLOWING:

- Disturbance of any surface dirt.
- Chunks of dirt on the ground that may have been dislodged from under the vehicle.
- Loose wires or strands of wire that are clean and probably 22 to 24 gauge.
- Look under, on top of, and on both sides of all four tires.
- Take off the hubcaps and check inside them and also the wheel locking bolts.
- Check the exhaust/muffler system for tampering, exhaust pipe for any inserted objects.
- Check the gasoline cap for possible tampering.
- Check inside the neck of the gasoline tank filler spout for foreign materials.
- With a flashlight and mirror, look under the bumpers; in the wheel wells; on top of the drive train; under the motor; and under/on top of the gasoline tank.

OPEN THE HOOD AND CHECK FOR THE FOLLOWING:

- Actuating devices that may be attached to the clutch, brake, accelerator or steering linkage.
- Signs of tampering with the air cleaner or equipment mounted on the firewall.
- Electrically initiated devices connected to power-operated equipment such as air conditioning, steering, and windshield wipers.
- Out of place or unusually clean wires.
- Parcels of any sort that could contain explosives.

OPEN A DOOR, INITIALLY ONE OTHER THAN THE DOOR TO BE USED BY THE PROTECTEE, AND CONDUCT AN INTERNAL SEARCH AS FOLLOWS:

- Check the interior thoroughly in a logical sequence, generally starting on the floor and working up.
- Check under the floor mats for pressure sensitive switches.
- Look under the front seats and lift and inspect under the rear seats.
- Check door panels for signs of tampering.
- Check under the dashboard for any loose or unusual wiring.
- Check the ashtray, cigarette lighters, rear seat radio speakers, vanity lights and dome light.
- Look under the dash for wires hanging down. Packages partially hidden under the front seat.

OPEN THE TRUNK AND CHECK THE FOLLOWING:

- Any wires that may be attached to the vehicle's brake lights or rear turn signals.
- Check behind and under the spare tire, the tool compartment, and the area behind the rear seat.

ONCE IT HAS BEEN DETERMINED THAT THERE IS NO DEVICE UNDER, ON, OR IN THE VEHICLE, TURN ON THE IGNITION.

AS A FINAL CHECK, OPERATE ALL DASHBOARD CONTROLS TO INCLUDE THE LIGHTS, RADIO, HORN, AIR CONDITIONER/HEATER, WINDSHIELD WIPERS, TURN SIGNALS, AND REAR WINDOW DEFOGGER.

ESTABLISH AND MAINTAIN CONSTANT SECURITY ON THE VEHICLE(S) TO INSURE CONTINUED INTEGRITY OF THE SEARCH.

Like Father, Like Sons

Otterbachers Have A History in EOD

The Naval Criminal Investigative Service (NCIS) has many interesting people associated with it.

For instance, Special Agent Wayne Goldstein and his family were featured in the April 1998 edition of the NCIS Bulletin. Before joining NCIS, Goldstein was a city police officer. Two of his brothers are still city police officers. His father is a retired fire department lieutenant, and two of his uncles retired as senior officers in law enforcement agencies.

Another family with a tradition of government and community service is that of Special Agent Dale Otterbacher Jr., Head of Firearms Training for NCIS.

Dale Jr. not only has eight years of U.S. Army experience as an Explosive Ordnance Disposal (EOD) technician, but he also comes from a family which includes others who have served in that elite and highly selective community.

His father, Dale Otterbacher, Sr., spent 20 years in the U.S. Air Force as an explosive ordnance disposal technician, then devoted another 20 years as a Florida State fire marshal, where he retired as a major.

DALE SR.

Dale Jr.'s next younger brother, Bruce Otterbacher, also enlisted in the U.S. Army and became an EOD technician. Bruce then went to work with the U.S. Secret Service as a protective technician, and is currently a special agent with the South Carolina State Law Enforcement Division (SLED).

In addition, Dale's next younger sister, Candy, is a dispatcher for a law enforcement and fire service, while his youngest brother, Ron, is a commander with the Orange County, Florida, Sheriff's Office and a former SWAT team member.

During his EOD career, Dale Jr. personally disarmed and destroyed numerous pieces of military ordnance and has performed render safe procedures (RSP) on many improvised explosive devices (IEDs), which are the most dangerous to disarm because they are so unpredictable.

***Dale Jr.**, kneeling at right, diffuses a live bomb containing seven pounds of C-4 in Orange County, Florida, as two other EOD technicians assist.*

Dale protected four U.S. Presidents while assigned to Secret Service details and taught bomb scene investigation and explosive safety to the members of the Bureau of Alcohol, Tobacco and Firearms (ATF) for three years at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia.

After eight years with the Army, Dale became a member of the Orange County Sheriff's Office in Orlando, Florida, where he became the head of the bomb and arson squad. Dale is a former member of the office's SWAT team and the recipient of the Orange County Sheriff's Office Medal of Valor.

Dale joined NCIS in 1985 and has served at the Los Angeles Field Office; Head of the Weapons Branch at NCIS Headquarters; the European Field Office in Naples, Italy, and the Resident Agency in Jacksonville, Florida, before coming to Headquarters, where he is a member of the Training Department.

LESTP Means "Total" Immersion

By Special Agent Shannon Zimmer
Criminal Intelligence Division

LESTP — If you have ever participated in the program, you know exactly what it means.

The Law Enforcement Spanish Training Program (LESTP) is held at the Federal Law Enforcement Training Center (FLETC), in Artesia, New Mexico. It is one of the most intensive, 10-day, total immersion Spanish law enforcement training programs around.

The 100-hour course is designed for law enforcement officers with little or no prior knowledge of the Spanish language. The objective of the course is to communicate with members of the Hispanic community during witness interviews and to recognize words and phrases that may indicate hostile intent.

With the rapid increase of the Hispanic community in the United States, the ability to communicate in Spanish has become critical. As a result, LESTP was developed in 1984, following a number of incidents in which law enforcement officers' lives were placed in jeopardy and in some cases lost, due to the inability to communicate key words or phrases with Hispanic speakers.

LESTP emphasizes learning arrest commands and the Miranda Warnings; recognizing dangerous street expressions in the Mexican, Puerto Rican and Cuban dialects; learning terminology for drugs and weapons; understanding cultural aspects of the Hispanic community; developing the ability to conduct simple field interviews; and being able to ask the who, what, why, where and when of law enforcement.

As one of 11 NCIS special agents who recently attended the LESTP course in September 1998, I can attest to the outstanding course and the dedication of the instructional staff.

During the first week, students take a pledge to the instructors, the class and themselves, speak only Spanish throughout the program. The students' typical day starts out with an hour lecture, several hours of drill classes, followed by lunch at the Spanish-speaking table.

Then there are more lectures, drill classes, an exercise section

"Bad words" *led to this apprehension during an LESTP training exercise. NCIS Special Agents Warren Lederberg, Chirstopher Cote and James Mulcrone subdued the "suspect" after recognizing something he said in Spanish that indicated he was about to reach for a weapon.*

Practical Exercises *are one of the ways LESTP instructors test their students. At left, Special Agent Annette Burton provides backup as Special Agent Shannon Zimmer apprehends a FLETC employee, who is playing the role of a suspect. In the top right photo, an instructor posing as a witness listens to Special Agent William Hammer, center, and Special Agent Zimmer, who are questioning him in Spanish.*

where students learn the Spanish alphabets (along with a lot of pushups for the letters they missed), more drill classes, situational action skits, and finally a cultural event, followed by homework. By the end of the day, students can barely say their names in English. But by the end of the program, students are communicating in Spanish.

At the end of the course, NCIS Special Agent John Weimer, who had no prior Spanish capability, was conducting felony car stops, field interviews, and participating in cultural skits in Spanish.

Another NCIS student, Special Agent Christopher Cote, had perfected his Spanish capabilities to the point where he was asked back to LESTP — not as a student, but as an instructor.

The course was a major success due to the outstanding efforts of LESTP Program Manager Elizabeth Truesdell; NCIS Special Agent JohnWizniak, who has been detailed to FLETC since January 1997; and guest instructors.

During the September class, the NCIS guest instructors were Special Agents Maria Rodriguez, Roberto Rivera, and Jody Diaz.

The instructors put in over 14 hours a day, performed numerous skits, dressed up in costumes, told students about their personal experience in dealing with Spanish and non-English speakers, and drilled students constantly with arrest commands and dangerous expressions.

All of this was done with one goal in mind - to give us fellow law enforcement officers the skills and ability to communicate in Spanish and survive.

NCIS Special Agent Awarded LESTP Associate Teaching Certificate

By Special Agent John Wizniak

Special Agent Maria Rodriguez has participated in the Law Enforcement Spanish Training Program (LESTP) in the capacitiy of Teacher's Assistant (TA) since April 1995, when she attended her first workshop. Since then she has been a TA in several classes. Her energy, enthusiasm, dedication and teaching skills have been an asset to the program.

In the most recent iteration of the class (LESTP-807) held between 14 and 24 November 1998, Maria helped in the coordination of the class and as the most experienced of the five guest TA's took on a leadership role in the meetings and in training of new TA's.

She was awarded a "Coordinator/Teaching Associate Certificate" by Elizabeth Truesdell, FLETC Program Manager for LESTP. Maria will be assisting in teaching the LESTP master classes in future classes.

Se habla Español agente especial?

Take a look at the following list of Spanish words and phrases and see if you can pick out the ones that might indicate trouble if you heard them "on the street." The answers are on page 35, at the end of the Bulletin Board section.

1. No hay de que
2. Cuidado
3. Correle
4. Cuetealo
5. Brincale
6. Calmese
7. Sientese
8. Pare
9. Lanchas
10. Agarralo
11. Matalo
12. Cual es su lugar nacimiento?
13. navaja
14. Pecas
15. Figalo
16. Llevatolo por medio
17. El caballo
18. Cuerno de chivo
19. La bufanda
20. Pescador
21. Mozo
22. El puente
23. Cocinero
24. Sigame
25. El jugo

NCIS Has Big Turnout For The CFC

This year's NCIS Headquarters Combined Federal Campaign (CFC) was different from previous campaigns.

To officially kick off the CFC Campaign, Mr. Benjamin Cumbo of the National Imagery and Mapping Agency spoke to NCIS Headquarters and Washington Field Office employees about how the CFC has helped his family. Mr. Cumbo's son, Benjamin, has the type of muscular dystrophy that causes gradual wasting of voluntary muscles, and usually requires use of a wheelchair later in life. Benjamin attended summer camp through a CFC agency, and last year he served as their national "ambassador."

The CFC kickoff ceremony focused on this year's CFC theme, "It all comes back to you."

The campaign was designed to be a fun, innovative, team-spirited vehicle that would give all NCIS employees in the Washington area the opportunity to participate in some way in raising funds for the more than 2600 local, national and international agencies participating in this year's campaign.

Fundraising events were proposed by NCIS employees from all NCIS disciplines and included a bake sale that raised $315; a picnic in Willard Park that raised $1,060; a breakfast that raised $645; a hot dog sale that raised $725; daily coffee sales; and a "Jail or Bail" event that raised over $800 in addition to providing a fun time for everyone involved.

As a reward for those employees who returned their pledge cards, Director David L. Brant and his staff donated their reserved parking places for weekly door prizes.

NCIS volunteers who have led the charge for the CFC are:

Marty A. Davis-Daniels, NCIS Washington, DC Coordinator, Economic Crimes; Mark N. Russ, NCIS 2nd Floor Team Leader; Benjamin A. Anderson, PC3, USN, Front Office; John J. Fencsak, Security Department; Mark O. Fox, Strategic Planning Group; Nancy L. Woolverton, Comptroller; Virginia L. Kirk, Public Affairs and Inspections; and John Daniels, III, Training Department.

***Mr. Benjamin Cumbo** is flanked by Director David L. Brant and Mr. Thomas F. Houston, Senior Advisor to the Director, after delivering the keynote address at the CFC kickoff at NCIS Headquarters.*

Deborah Wells, Team Leader, Counterintelligence Department; Richard A. Skelton; Mark N. Russ; Andrea M. Hoskin; Lisa R. Boice; Stewart R. Wilson; and Thomas Dean, IS3, USN.

Michael G. Sullivan, Team Leader, Criminal Investigations; Anna M. Keip; Mimi C. Band; Carla B. Pinto; Shawn E. Anderson, Team Leader, 3rd Floor, Computer Investigations; Betty J. Callis, Law Enforcement and Physical Security; Carzena M. Sawyer, Career Services; Mark R. Pottebaum, Computer Investigations and Operations; and Lisa A. Beverly, Information and Physical Security.

Grace H. Barcia, Team Leader, Information Systems; Mary E. Neely; Randy J. Lambert, RM3, USN; Donna M. Klein; Terrance W. Lauer; Lois L. Buckmaster; Pamela F. Robinson, Team Leader, DoN Central Adjudication Facility; Kay R. Hawkins; and Regina A. Proctor.

Claude R. Baldwin, Team Leader, NCIS Washington, DC, Field Office; Deborah I. Reese; and Roberta J. Helmus

Special Events: Tammy L. Paulus, Training Department, and Kelli C. Scott, Investigative Support Program.

NCIS employees *in the atrium of Headquarters watch a CFC video presentation, at left. A performance by a string quartet, above, was another attraction at the CFC kickoff. Mr. Peter Enchelmeyer of the Security Department arranged for the quartet to appear at the CFC kickoff.*

Below, Team Leader Deborah Wells, second from left, oversees the fundraiser picnic that raised over $1,000 for the CFC. Keyworkers helping her are Lois Buckmaster, center, Lisa Boice, second from the right, and Anna Keip, at right.

In the bottom left photos, NCIS CFC Coordinator Marty Davis-Daniels, at left, cooks sausages, and Kelli Scott , at right, helps serve food at the breakfast which raised over $600 for the CFC. On November 12, volunteers led by Davis-Daniels had a hot dog sale at lunch and raised another $725.

Combined Federal Campaign

Civilian Meritorious Service Medals *were presented by Capt. S.A. Turcotte, left, to Special Agents James Lennon and Valerie Thompson. Standing next to Thompson is Special Agent in Charge Brian Stamper, who is also standing at left in the photo at right. Mr. Leland Roberts, center in the photo at right, presented special act awards to Special Agent Jerry Whitacre, second from left, Special Agent Thompson, and Mr. Robert Thompson, at right.*

Members Of Jacksonville Task Force On Workers' Compensation Honored For Their Achievements

Rear Adm. Kenneth Belisle, Commander Naval Base Jacksonville, Florida, awarded Meritorious Civilian Service medals to **Special Agents James Lennon and Valerie Thompson**.

The medals were presented on behalf of Rear Adm. Belisle on October 1, 1998, by **Captain S.A. Turcotte**, Commanding Officer, Naval Air Station (NAS) Jacksonville.

Lennon and Thompson were part of an ongoing Workers' Compensation Operation conducted jointly by the Mayport Field Office, the U.S. Attorney's Office, and the NAS Jacksonville Human Resources Office (HRO).

The Meritorious Civilian Service Medal was presented to Lennon for his efforts to combat workers' compensation abuses from October 1996 to September 1998. His efforts resulted in the successful prosecution of three Department of the Navy employees by the U.S. Attorney's Office in Jacksonville. The investigations resulted in $1.7 million in direct savings to area commands and the Commander in Chief Atlantic Fleet.

Thompson was awarded the Meritorious Civilian Service Medal for her efforts to detect and thwart workers' compensation abuses from April 1997 through January. Her expertise enhanced the coordination of subject matter experts of the Department of Labor, area commands, and the Human Resources Office at NAS Jacksonville, and helped realize over $4 million in direct savings to area commands.

Captain Jan C. Guadio, Commanding Officer, Naval Station, Mayport, Florida, presented special act awards to NCIS **Special Agents Valerie Thompson and Jerry Whitacre**, and **Injury Compensation Program Administrator Robert Thompson** of the Human Resources Office. The awards were presented by Leland Roberts, Executive Director, and Marcus Hill, Manpower Management, Naval Station Mayport on October 1, 1998.

The award was presented for their outstanding performance as members of the Workers' Compensation Task Force, which helped save Naval Station Jacksonville $1.8 million.

Director David L. Brant presented **Intelligence Analyst John Beattie** with the Department of the Navy (Don) Superior Civilian Service Medal and awarded the DoN Meritorious Civilian Service Medal to **Special Agent Stewart R. Wilson** during a ceremony held at NCIS Headquarters in November.

The citation presented to Beattie read as follows: "For superior civilian service as the primary Intelligence Analyst assigned to the Robert C. Kim Espionage Investigation Task Force from January to October 1996. Mr. Beattie was assigned the arduous task of analyzing voluminous numbers of technical surveillance video tapes to determine Robert C. Kim's methodology of transferring Unites States government documents to a foreign power.

"Mr. Beattie persisted with tenacity and uncovered Robert Kim's intricate system of spying and overall espionage methodology. In fact, Mr. Beattie became so proficient at what he did, he was able to predict which classified documents Kim would attempt to transfer; Mr. Beattie's predictions were always accurate, which streamlined the coordination process with the originators of the documents.

"In addition, Mr. Beattie's intricate knowledge of the case facts was unsurpassed by any other members of the team, and it would be fair to acknowledge that he had authored the prosecutive summaries.

"Throughout this complex investigation, Mr. Beattie maintained a positive demeanor and provided the case agents timely leads and analytical insights, which contributed to the thoroughness of the investigation. It was Mr. Beattie's unselfish devotion to his duty which led to the successful prosecution of Robert C. Kim."

The citation presented to Wilson read: "For meritorious service to the Directorate of Intelligence, United States Transportation Command, Scott Air Force Base, Illinois, between July 1995 and August 1998. Mr. Wilson's leadership and vision greatly improved the counterintelligence support throughout the command and provided key building blocks to the command's Force Protection program.

"Mr. Wilson vastly expanded the capabilities of USTRANSCOM's counterintelligence team, building its billet strength by 400% and coauthoring the command's Force Protection Operations Steering Group Charter. He personally briefed and advised the Commander in Chief and Deputy Commander in Chief on issues of critical importance to the safety and security of USTRANSCOM forces.

***Director David L. Brant** presents medals to Intelligence Analyst John Beattie, in the top photo, and Special Agent Stewart R. Wilson, above.*
(Photos by Gary M. Comerford)

"By closely coordinating with federal law enforcement organizations, military services, theater commands and national intelligence agencies, Mr. Wilson engaged every possible resource to ensure the safe planning, preparation, and operation of USTRANSCOM forces while they transported personnel and material throughout the globe."

Special Agent Bruce R. Washawsky of the Hawaii Field Office was among a group of federal, state, local law and military law enforcement officers presented with the "Top Cops" Award at the 14th Annual Law Enforcement and Security Appreciation

Luncheon held October 8 at the Sheraton Waikkiki Hotel. The event is sponsored by the Council of Police and Private Security (COPS).

Warshawsky was honored for his super investigative efforts in a "Cold Case" involving the 1985 death of a five-year-old girl who was the daughter of an active duty Navy member. When the case was reopened years later, Warshawsky doggedly pursued investigation. As a result of his efforts, a suspect has been indicted, arrested and is currently awaiting trial.

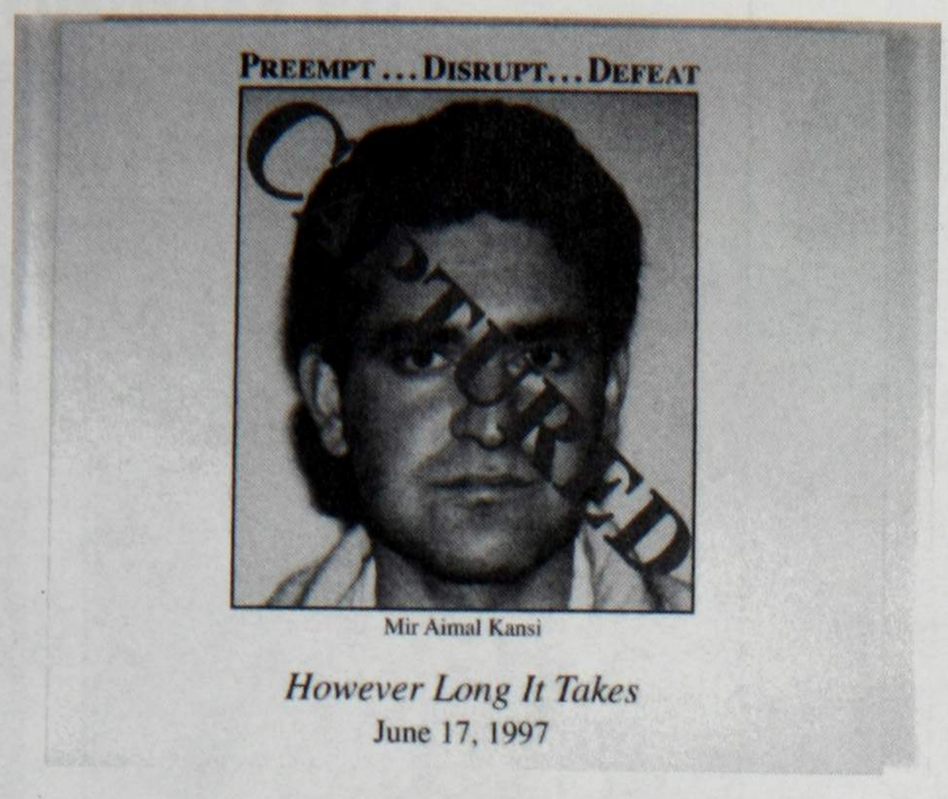
Washawsky was also responsible for recently solving a rape of a wife of an active duty Navy member, which occurred in base housing in 1992.

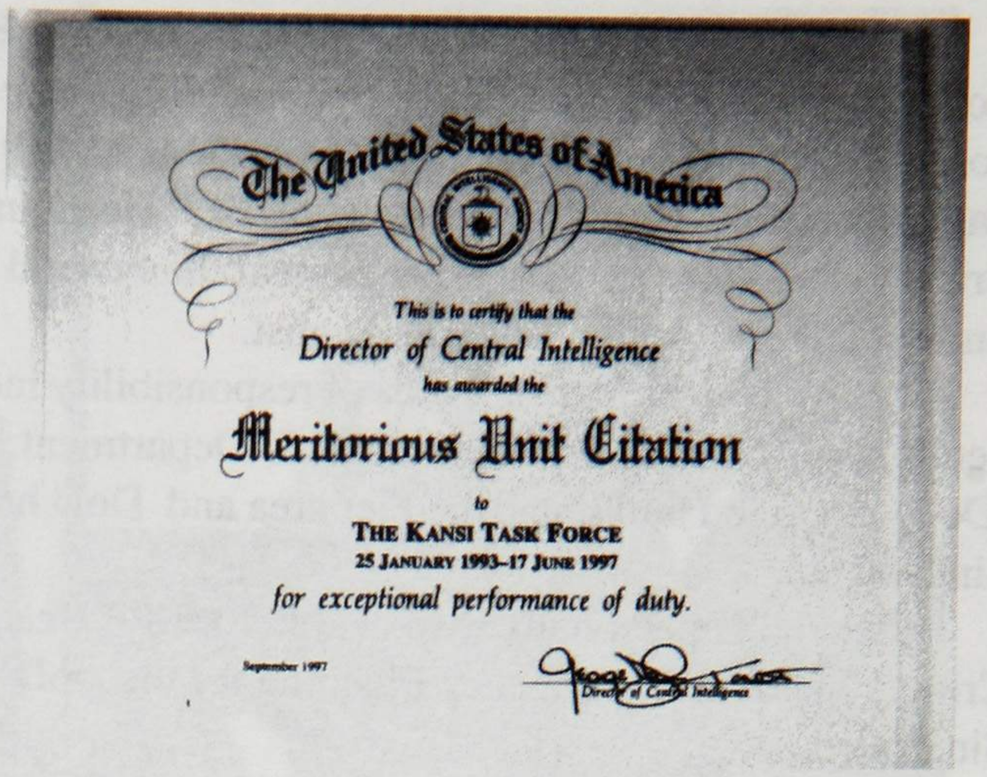
***Lt.Cmdr. Gordon Sheek, USN**, is presented with the Navy Commendation Medal by Special Agent Al Billington of the Middle East Field Office in Bahrain during a ceremony held on September 2, 1998. Sheek, who was formerly assigned to the NCIS Law Enforcement and Physical Security Department, supervises more than 120 security personnel at the Navy facility in Bahrain.*

***The "38th Parallel" in Korea** was one of the places Director David L. Brant visited on his trip to the Far East earlier this year. In the top photo, Director Brant looks across the border at North Korea.*

In the photo above, an Army captain briefs Director Brant, Senior Advisor Tom Houston, and Assistant Director for Administration Franz Schwarm during a visit to the building where the treaty ending the Korean War were negotiated.

***Special Agent Brian MacPhee**, right, is congratulated by Director David L. Brant during a ceremony at the NCIS Resident Agency in Seoul, Korea. Director Brant presented MacPhee with a letter of commendation in recognition of his outstanding counter drug work at his previous assignment in Boston, Massachusetts. MacPhee is currently assigned to the Resident Unit in Pusan.*





NCIS Special Agent Paul Sparks *attended an awards ceremony at the Central Intelligence Agency (CIA) Headquarters on September 18, 1998, where he and fellow CIA and FBI officers were honored with a Meritorious Unit Citation for their involvement in the capture of Mir Aimal Kansi. Kansi shot and killed two CIA officers and wounded several other officers outside CIA Headquarters on January 25, 1993 and immediately fled overseas. Kansi was apprehended on June 17, 1997 at an overseas location as the result of a joint CIA/FBI investigation. Sparks was detailed to the Director of Central Intelligence Counterterrorist Center (CTC), CIA Headquarters, during January 1994 - September 1998 and worked on the Kansi rendition while assigned to the CTC Special Projects Branch. Shown above is a copy of that award encased in clear plastic.*

The Singapore Resident Agency *was visited by Director David L. Brant, Assistant Director Franz Schwarm and Senior Advisor Tom Houston in September.*

Director Brant and his party received an in-brief by NCIS specia agents regarding operations in South East Asia, then proceeded to Singapore Police Headquarters for an official program in honor of the Director's visit. Following a series of briefings about the Singapore Police Force and crime in Singapore, Director and his party dined at the Thanying Restaurant as guests of Singapore Commissioner of Police Khoo Boon Hui and members of his senior staff.

Commissioner Khoo presented Director Brant with a specially cast Selangor Pewter Plate depicting scenes of the Singapore Police Force, engraved in honor of Director Brant's visit. Director Brant presented Commissioner Khoo a miniature set of ONI, NIS and NCIS badges encased in plastic. In the top right photo, Assistant Director Schwarm, Senior Advisor Houston and Director Brant meet with Commissioner Khoo.

NCIS hosted **Police Superintendent T. Raja Kumar**, Commander, Ang Mo Kio Police Division, Singapore Police Force (SPF) and **Assistant Superintendent (ASP) Daniel Tan**, Operations Planning Department, SPF Headquarters, for a Crisis Management Training Program at the Federal Law Enforcement Training Center in August.

Superintendent Kumar's area of responsibility includes the Sembawang Wharfs area holding U.S. Department of Defense (DoD) occupied buildings, the Pier area and DoD housing in Singapore.

ASP Tan is personally responsible for SPF Headquarters Critical Incident Contingency Planning for the DoD presence in Singapore.

Superintendent Kumar and ASP Tan were the first ever Singapore Police Officers to attend a course at FLETC. The training was also attended by **Supervisory Special Agent Stephen Smith of the** NCIS Resident Agency Singapore .

Under the 1990 United States - Singapore Memorandum of Understanding, the SPF are vested with primary responsibility for the protection of DoD facilities and 600 U.S. DoD permanent personnel in Singapore, as well as over 150 USN and MSC port visits and liberty parties each year.

Kumar and Tan are key NCIS counterparts for Force Protection planning and response in Singapore. This Joint Crisis Management training experience will directly benefit ongoing NCIS Force Protection Crisis Management planning and exercise programs with the SPF.

The course was arranged by **Special Agent Leonard Lawing**, NCIS FLETC representative; **Special Agent Tom Betro**, NCIS Headquarters, Pacific Division Chief; **Special Agent Al Chester**, Training Division; and **Assistant Special Agent in Charge Michael Barrett** of the Far East Field Office.

***From left to right**, are Special Agent Leonard Lawing, Superintendent T. Raja Kumar, Assistant Superintendent Daniel Tan, and Special Agent Stephen Smith.*

Living Legend

Naval Criminal Investigative Service Virginia

SPECIAL AGENT JOANNE JENSEN

SA Jensen, a 13-year NCIS veteran, is nationally recognized for her ability to obtain confessions, develop reliable informants, and for her tenacity in conducting investigations. According to her colleagues, she has an uncanny ability to zero in on the truth. Among the cases that make up her 99% conviction rate, SA Jensen and her partner developed a circumstantial case against a murderer that resulted in the first guilty verdict in U.S. history without a body and with no physical evidence. "Perfect Crime", a USA Network movie, was based on this investigation. Special Agent Jensen makes an additional contribution — she is singularly responsible for helping many of her informants start new crime free lives.

NLEOMF Officer of the Month January 1997

***Special Agent JoAnne Jensen** is featured as the January 1999 "Living Legend" on the National Law Enforcement Officers Memorial (NLEOM) calendar.*

Yokosuka PD Hosts NCIS

Senior Superintendent Yutakata Tazaki , Chief of the Yokosuka Police Department, presents Director David L. Brant with a memento during his visit to the Far East. Accompanying Director Brant were Assistant Director Franz Schwarm, Senior Advisor Tom Houston, and Special Agent in Charge Tom Orzechowski of the Far East Field Office.

Director Brant Visits Yuma

The NCIS Resident Agency in Yuma, Arizona, was visited by Director David L. Brant earlier this year. From left to right are Special Agent Michael Burke, who is also a Marine CID agent; Special Agent B.J. Yankosky; Investigative Assistant Anna Adams; Director Brant; Special Agent Cody Hatch; and Special Agent Eric Chapman.

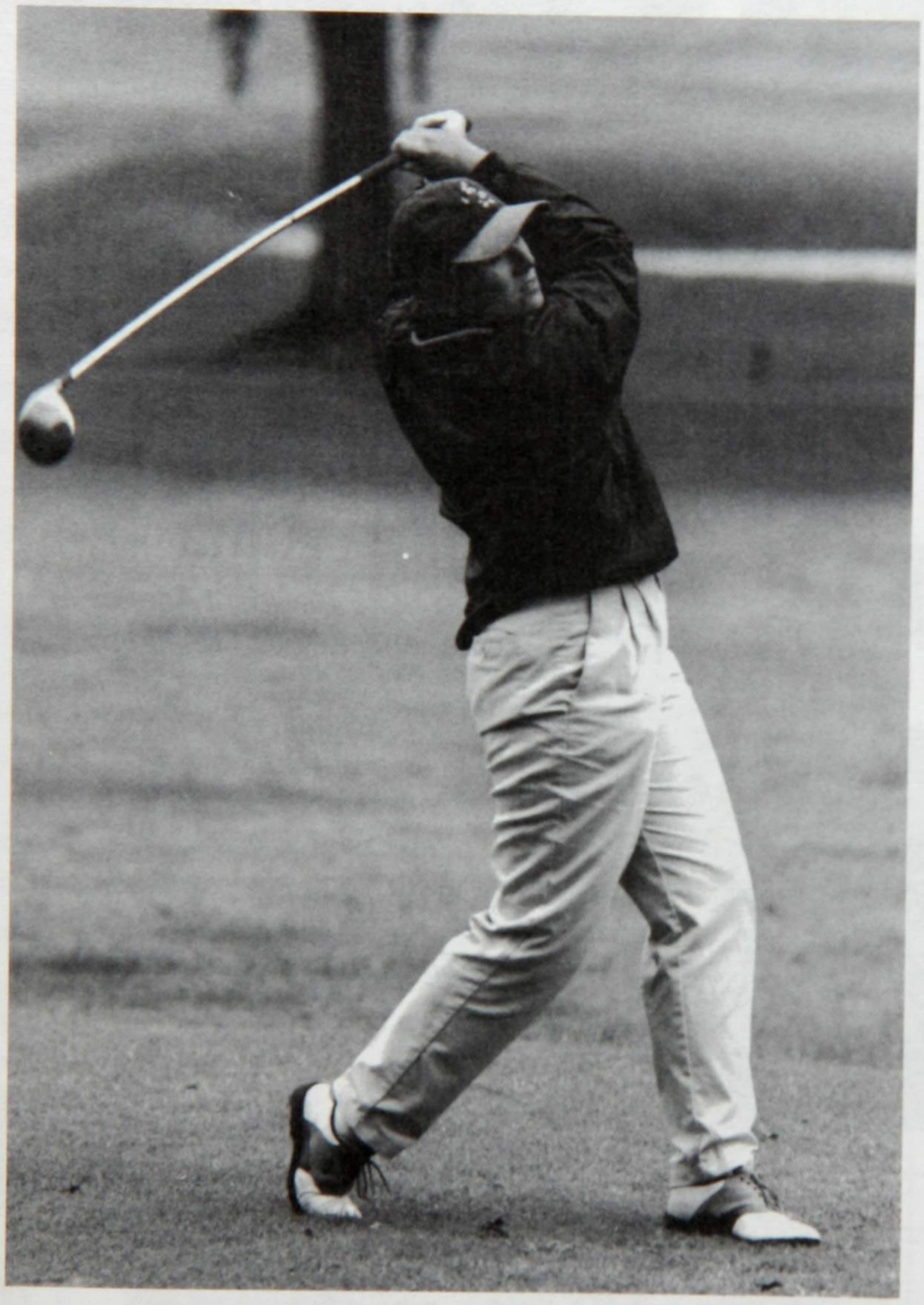
Se habla Español agente especial?

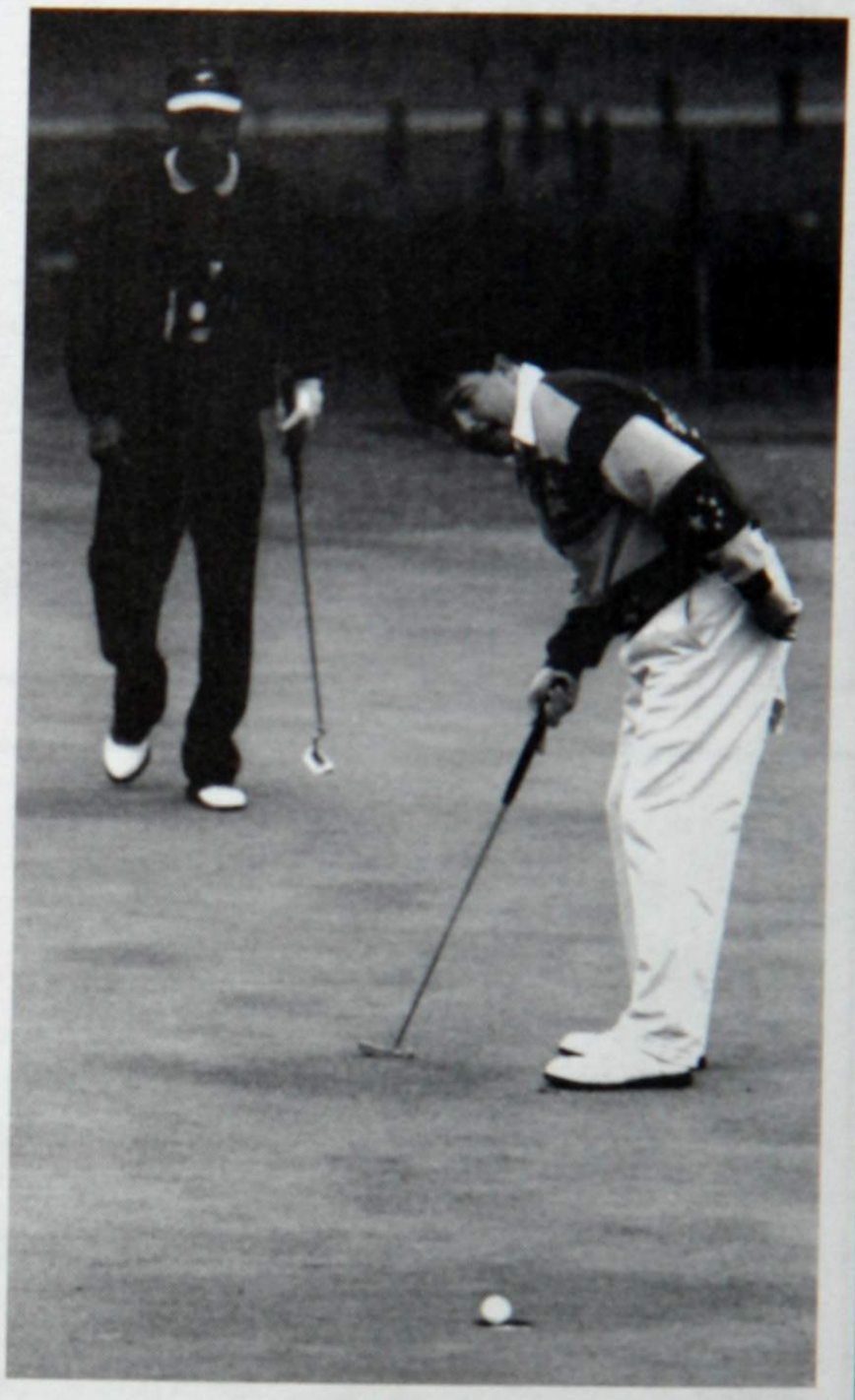
Here are the answers to the list on page 27.

1. No hay de que. - You are welcome. 2. Cuidado - Be careful. 3. Correle - Run. 4. Cuetealo - Shoot him. 5. Brincale - Hit him. 6. Calmese - Calm down. 7. Sientese - Sit down. 8. Pare - Stop. Lanchas - small boats. 10. Agarralo - Grab him. 11. Matalo - Kill him. 12. Cual es su lugar nacimiento? - What is your place of birth? 13. Navaja - switchblade 14. Pecas - freckles 15. Figalo - Stab him. 16. Llevatolo por medio - Run over him. 17. El caballo - slang term for heroin (literally "horse") 18. Cuerno de chivo - the slang term for an AK-47 (literally "goat's horn") 19. La bufanda - scarf 20. Pescador - fisherman 21. Mozo - waiter 22. El puente - bridge 23. Cocinero -cook 24. Sigame - Follow me (singular). 25. El jugo - fruit juice

Sports

NCIS Holds Annual Tourney At Quantico



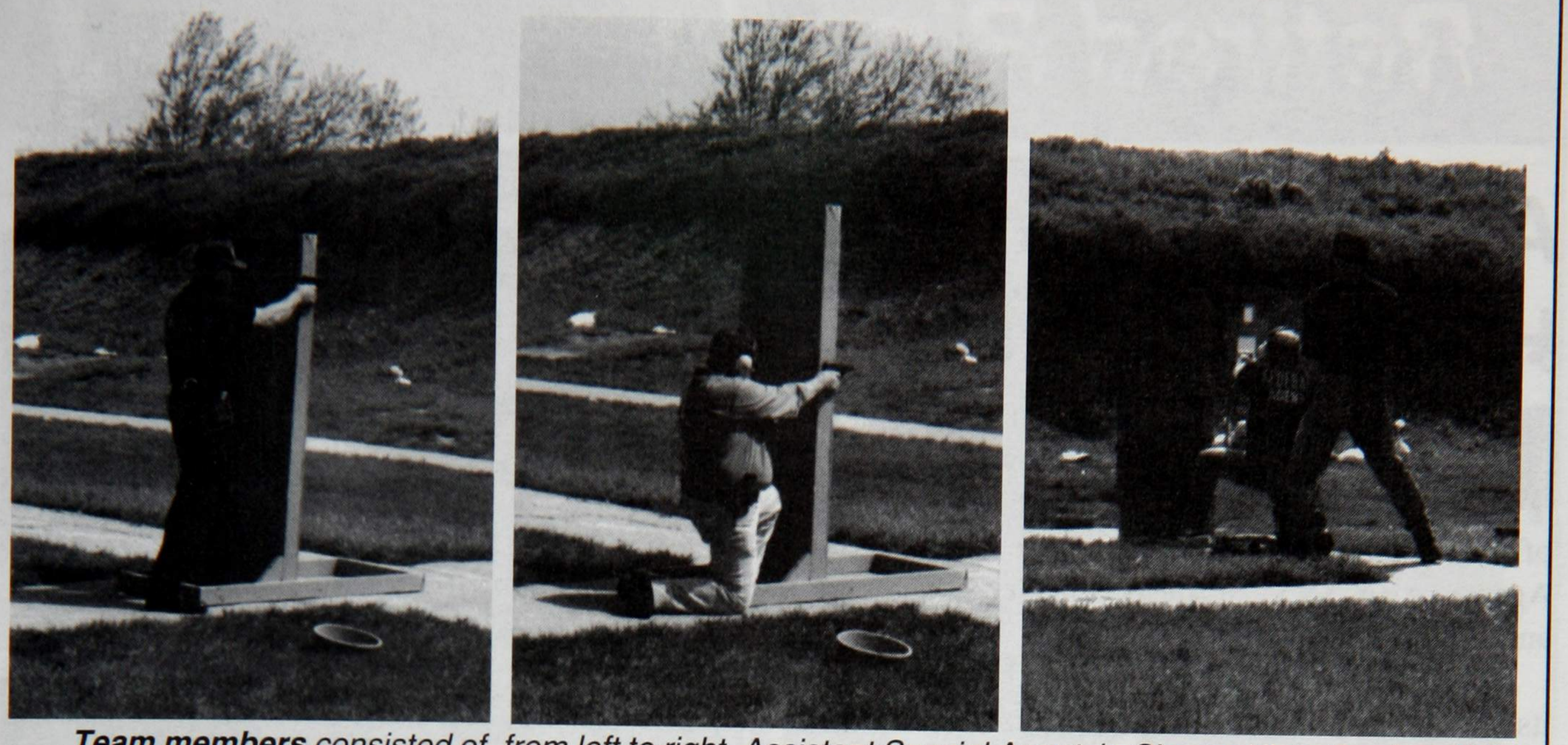


(Photos by Gary M. Comerford)

***Lt. Stephanie Smart, JAGC, USN**, above, won the award for the longest drive at the NCIS Annual Golf Tournament on October 9. Smart, who is assigned to NCIS Headquarters, is transferring to Norfolk in January.*

Eighty-eight federal, state and local law enforcement representatives participated in the event, which was held at the Medal of Honor Golf Course at the Marine Corps Base in Quantico, Virginia.

In the top right photo, NCIS Special Agent John Tigmo sinks a put as Special Agent Ron Casey looks on. At right, a representative from another agency lofts a shot.



Team members *consisted of, from left to right, Assistant Special Agent in Charge Klain Garriga, NTC Great Lakes Chief of Police Jim Goldman, and Special Agent Mike Keleher.*

NCIS Great Lakes Combined Pistol Team Places Ninth In Illinois Tactical Officers Association Shoot

A combined team consisting of two members of the NCIS Resident Agency Great Lakes Office and the Chief of Police for Naval Training Center (NTC) Great Lakes, Illinois, recently competed in the 1998 Illinois Tactical Officers Association Combat Handgun Competition.

The statewide competition is open to federal, state and local officers and is held at several locations throughout the state.

Assistant Special Agent in Charge Klain Garriga, Special Agent Mike Keleher and NTC Great Lakes Chief of Police Jim Goldman joined forces to tackle the "Running and Gunning" on two different courses of fire.

The match simulates real life combat shooting and features running, shooting, reloading and use of cover to reinforce safe tactics and accuracy. Each individual score is measured by speed and accuracy.

The NCIS team placed ninth overall in the competition and enjoyed meeting some of the best combat shooters in the state. Special Agent Keleher was also the overall winner of a side match sponsored by the Chicago FBI office.

NCIS Reservist Competes On TV Show "Jeopardy"

Lt.Cmdr. Tom Gould, a Naval Reservist assigned to NCIS Headquarters Unit 0166, was a contestant on a segment of the popular television game show Jeopardy in September.

Gould flew to Los Angeles for the taping in July. As luck would have it, one of the categories was "Intelligence", and he was faced with questions about moles and the Enigma machine. Of course he had to make sure that all of his responses were phrased in the form of a question.

Although he fought the good fight, he finished a close second to a defending two-time champion. For his efforts, Gould won an all expenses paid vacation to Barbados.

As a Naval Reservist, Gould serves as watch officer in the Navy's Antiterrorist Alert Center at NCIS Headquarters. In his civilian life, Tom is a counterterrorism analyst at the Defense Intelligence Agency.

ARNISSA Reunion Has Good Turnout

More than 60 retired agents and their spouses gathered in Atlantic City, New Jersey, on September 28-30, 1998 for the Association of Retired Naval Investigative Service Special Agents (ARNISSA) Northeast Chapter's Reunion and Convention.

ARNISSA currently has over 700 members on its roster. "In addition to retired agents, that includes the spouses of deceased agents and some people who, although they didn't retire from NIS, did significant time with us, either as agents or military members," said ARNISSA President and former NIS Director J. Brian McKee.

Among those attending the reunion were NCIS Director David L. Brant, who was accompanied by Assistant Director Vic McPherson (Government Liaison and Public Affairs); Assistant Director Thomas Fischer (Inspections); Mr. Tom Houston, Senior Advisor to the Director; and Special Agent in Charge Roni McCarthy of the Northeast Field Office. All were present for the ARNISSA banquet, which was held Tuesday evening, September 29.

Following the banquet, Director Brant addressed the members, and discussed recent events in NCIS as well as some of the new programs and prospects for the future.

"Everyone felt very confident that the organization is in good hands and that NCIS is on solid ground," McKee said. "And Dave's efforts the past couple of years to bring the retirees closer to the active organization are very much appreciated."

The Third Annual National ARNISSA Reunion and Convention is scheduled for March 11-14, 1999 at the Handlery Hotel and Resort in San Diego, California. The event will include golf and tennis tournaments, along with an ocean dinner cruise and shopping trips.

Reservations must be handled on an individual basis by contacting the hotel directly. The deadline for reservations is February 11, 1999.

***Retired Special Agent Pete Reilly**, Retired Director J. Brian McKee, Special Agent in Charge Roni McCarthy, Director David Brant, and Senior Advisor Tom Houston, shown in the top photo, were seated at the same table for the ARNISSA banquet. In the middle photo, Director Brant presents an award to Retired Special Agent Jimmy Jones, while in the bottom photo Retired Special Agent Bob Panico and "Soon to be Retired" Assistant Director Vic McPherson pose for a photo.*

Former Directors Return to Headquarters

Six former directors *gathered at NCIS Headquarters in September 1998 as guests of Director David L. Brant. Following a series of morning briefings, including an update on the NCIS Computer Crimes Investigations and Operations Department, the former directors joined Director Brant for lunch and then gathered outside Headquarters for a group shot.*

Shown above, from left to right, are Mr. Sherman Bliss (1980-1981), Mr. Earl Richey (1976-1980), Mr. Charles R. Lannom (1992), Director Brant, Mr. Bert Truxell (1982-1984), Mr. Jack I Guedalia (1984-1986), and Mr. J. Brian McKee (1986-1990).

This is the second year in a row the former directors have gathered at NCIS Headquarters at the invitation of Director Brant. The meetings not only allow the retired agents to learn about new investigative methods and trends, but also allows NCIS to benefit from their knowledge and years of law enforcement experience.

(Photo by Gary M. Comerford)

TOP TWENTY LIST

The NCIS "Top Twenty List" includes the top 20 professional support staff personnel in terms of length of service. The "Top Twenty" as of September 30, 1998, are listed below:

	Name	Duty Station	NCIS Date
1.	Conover, Jean S.	Washington, DC	October 19, 1964
2.	Neely, Mary E.	Washington, DC	January 11, 1965
3.	Jones, Charles F.	Norfolk, Virginia	June 6, 1966
4.	Lee, Brenda Sue	Washington, DC	August 22, 1966
5.	Scroggie, Linda L.	San Francisco, California	October 13, 1968
6.	Hooker, Nancy Gayle	Mayport, Florida	May 12, 1969
7.	Kelly, Elaine B.	Pensacola, Florida	July 1, 1971
8.	Hamand, Jerilynn A.	San Diego, California	March 27, 1973
9.	Allport, Sandra D.	Washington, DC	August 5, 1973
10.	Green, Donna C.	Washington, DC	June 24, 1974
11.	Cross, Deborah Ruth	Memphis, Tennessee	August 5, 1974
12.	Rommes, Barrie Ann	Pensacola, Florida	August 12, 1974
13.	Lucy, Donna Jean	St. Louis, Missouri	December 2, 1974
14.	Anderson, Mary Ann	Washington, DC	March 3, 1975
15.	Kohler, Nancy Leigh	San Diego, California	April 7, 1975
16.	Griffith, David R.	London, England	July 14, 1975
17.	Carter, Jan Cook	New River, North Carolina	September 2, 1975
18.	Parham, Deborah L.	Norfolk, Virginia	October 20, 1975
19.	Reynolds, Janet D.	Washington, DC	November 17, 1975
20.	McGuinn, Gary A.	Washington, DC	March 3, 1976

Law Enforcement Liaison

***Retired Sheriff John Bunnell**, who appears on the television series "Cops" as well as another well-known law enforcement program, is flanked by Assistant Special Agent in Charge Grant McIntosh and Assistant Special Agent Charlie Strickland.*

Bunnell, who flew in from Hollywood, was the guest of the Kings Bay Resident Agency, which was sponsoring its Third Annual Law Enforcement Submarine Embarkation Cruise. Bunnell, along with 13 federal, state and local law enforcement officer s from Georgia and Florida, took part in the two-day event, which was hosted by the USS Wyoming (SSBN 742).

***Police Chief Jerry Hinton** of Brunswick, Maine, at left in the photo below, and Special Agent Ray Kessenich of the Brunswick Resident Agency are shown onboard the U.S. Coast Guard Cutter Jefferson Island (WPB-1340) during an escort for the Coast Guard tall ship Eagle (in the background) . The event took place in August in Casco Bay Harbor off the coast of Portland, as a precursor for "Op Sail 2000."*

PLANK OWNERS' LIST

The "Plank Owners' List" showing the top 25 NCIS special agents in terms of length of service. The "Plank Owners" as of November 30, 1998, are listed below:

Name	Duty Station	NCIS Date
1. Laing, William D.	Philadelphia, PA	May 17, 1965
2. Whidden, Marshall T.	Pensacola, Florida	May 24, 1965
3. McPherson, Victor H.	Washington, DC	August 26, 1968
4. Gerwerth, Joseph F.	Norfolk, Virginia	December 18, 1972
5. Spears, Stephen E.	Stuttgart, Germany	June 17, 1973
6. Clookie, Wayne D.	San Diego, California	November 23, 1973
7. Bruggeman, Michael D.	Washington, DC	November 26, 1973
8. Kelly, Lauchlin A., III	Washington, DC	January 7, 1974
9. Landin, Joseph C.	Norfolk, Virginia	May 13, 1974
10. Mugglesworth, Charles D.	Frankfurt, Germany	June 24, 1974
11. Boley, Thomas F.	Washington, DC	July 22, 1974
Coyle, Charles K.	Pensacola, Florida	July 22, 1974
Gehri, John R.	Jacksonville, Florida	July 22, 1974
Rossman, Harlan	Washington DC	July 22, 1974
15. Nigro, Robert M.	Washington, DC	July 25, 1974
16. Carman, Ray	Washington, DC	July 26, 1974
Jester, John	Norfolk, Virginia	July 26, 1974
Logan, Gary	Jacksonville, Florida	July 26, 1974
19. Bradley, Vaughn M.	Baltimore, Maryland	July 29, 1974
20. Smart, Bruce A.	San Diego, California	July 31, 1974
21. Zane, Alexander P.	Washington, DC	August 1, 1974
22. Bruce, Donald R.	Pensacola, Florida	August 5, 1974
23. Harris, Michael W.	Orlando, Florida	August 6, 1974
Kauffman, Frank	Washington, DC	August 6, 1974
Reno, Charles	Los Angeles, California	August 6, 1974

RETIRED

The following is a list of NCIS personnel who have retired since October 1, 1998:

Name	Location	Retired
SA Albert Maretta	Pensacola, Florida	October 31, 1998
SA Gerald Nance	Washington, DC	December 3, 1998

The address for the NCIS Web Site is:

www.ncis.navy.mil

NCIS Attends IACP Conference

Police Chief Dennis Mook *of the Newport News, Virginia, Police Department, stands between Special Agent in Charge Wayne Bailey of the Norfolk Field Office and Director David L. Brant in the top photo. Director Brant had just presented Chief Mook with the first NCIS "Law Enforcement Partnership Award." The presentation was made during the NCIS breakfast held on October 19, during the International Association of Chiefs of Police (IACP) annual convention in Salt Lake City, Utah.*

The new NCIS display made its debut at the IACP conference. Special Agent Wayne Jones, left, and Special Agent Sheri Rostodha, right, take their turns at the display greeting conference attendees.

(Photos by Tom Houston)

Naval Criminal Investigative Service
Washington Navy Yard Building 111
716 Sicard Street S.E.
Washington, D.C. 20388-5397

Address Correction Requested