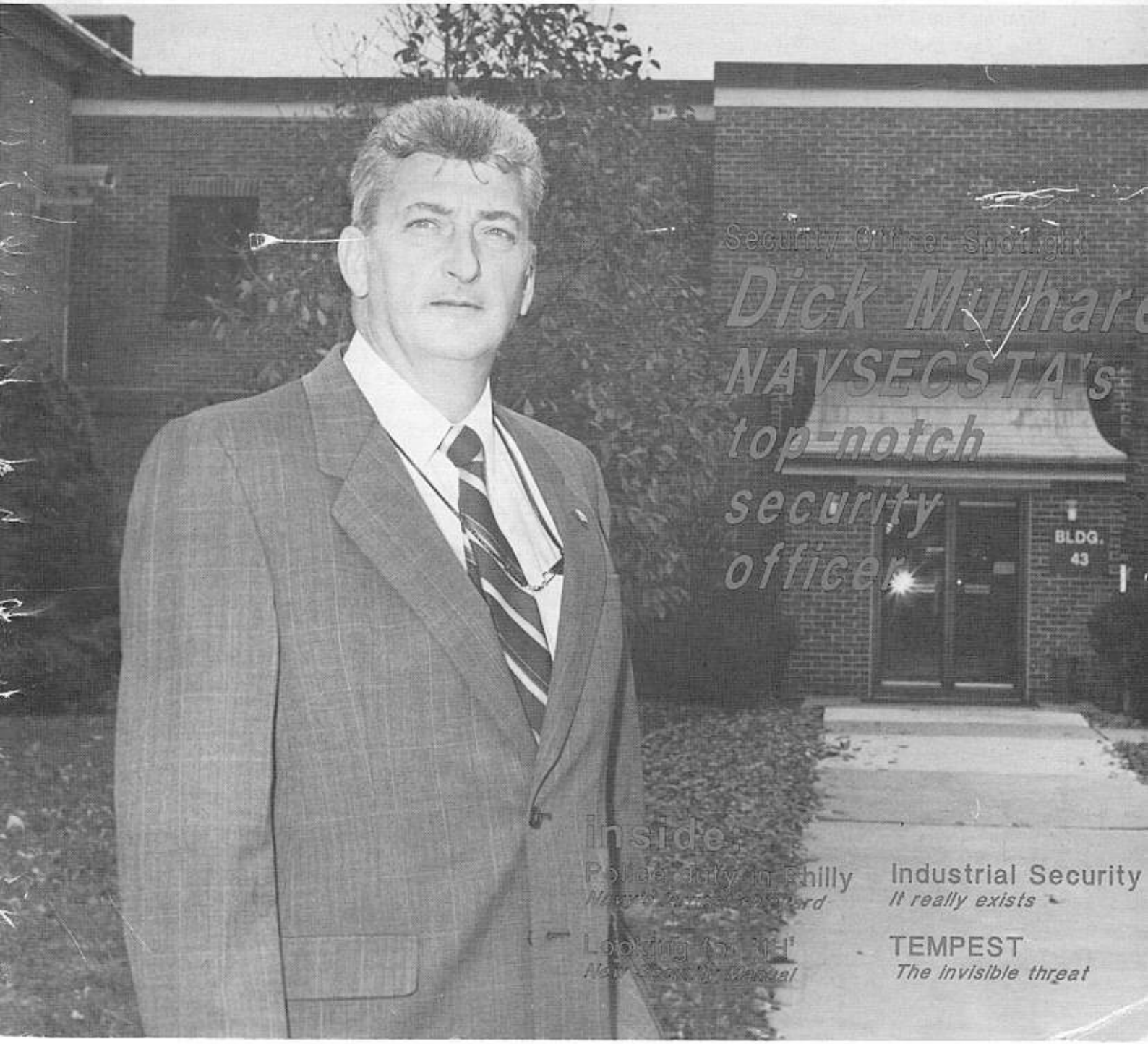
Sentry

For the Navy Security community

Vol. 1, No. 6 Fall 1988/Winter 1989

Jungle patrol
page 35



Security Officer Spotlight

Dick Mulhare
NAVSECSTA's top-notch security officer

Inside:

Sentry
For the Navy Security community

Vol. 1 No. 6 Fall 1988/Winter 1989

Special features

News & Features

Departments

From the editor:

Since last issue, I've received a lot of positive response from the fleet concerning the changes and expansion of *Sentry*. This issue reflects even more changes, expanding into areas of **Industrial Security** and **Technical Security**, and the growing **Legal Issues, Information Security** and **Personnel Security** sections.

The command is also growing and changing. As of 1 October 1988, we are now the Naval Investigative Service Command (NISCOM), and have a new headquarters building to go with the new name. Our new location is at the Washington Navy Yard, Building 111. This move has not affected our mailing address with the exception of a slight change to the +4 zip code. Mail going to Code 24 (Law Enforcement & Physical Security Programs) will go to 20388-5024. Submissions for *Sentry* should also go to this address. Mail for Code 21 (Information and Personnel Security) should be addressed to 20388-5021. Our move is still in progress so allow extra time for mail to catch up with us.

New point of contact phone numbers will be provided next issue.

Sentry, the newspaper of the Naval Investigative Service Command (NISCOM), is an authorized publication for all Navy and Marine Corps personnel involved in law enforcement and security, issued quarterly from NISCOM Headquarters. Opinions expressed are not necessarily those of the government of the United States, the Department of Defense, nor the Department of the Navy. Reference to regulations, orders and directives is for information only and does not by publication herein constitute authority for action. Original articles, information and photographs may be submitted to Sentry Editor, Naval Investigative Service Command Headquarters, Code 24J, Washington, DC 20388-5024. Autovon: 288-9096; commercial: (202) 433-9096.

Commander, Naval Investigative Service Command
Rear Adm. John E. Gordon, USN, JAGC
Deputy Commander, Naval Investigative Service/Plans
Col. Wayne A. Coomes, USMC
Deputy Commander, Naval Investigative Service/Operations
J. Brian McKee
Director, Law Enforcement & Physical Security Programs
James A. O'Hara
Assistant Director, Information & Personnel Security Policy
Charles V. Page
Sentry Editor-in-Chief
JO1 John S. Verrico, USN

FROM THE COMMANDER

Making an impact

Rear Adm. John E. Gordon

In the last issue of *Sentry*, I talked about doing more with less. Now I want to expand on that theme and talk about having an impact in the performance of our work.

Having an impact means that we are getting the expected, or greater, return for our efforts. It does not mean just "getting the job done." In terms of the many security and investigative disciplines we represent at the Naval Investigative Service Command (NISCOM), it means better trained security people because we had an impact on the quality and availability of the training. In the fleet, it means you attained command-wide security awareness -- full time. It means a successful Inspector General inspection because you knew the regulations, implemented effective and efficient security procedures, detected security vulnerabilities and corrected them before a breach of security could take place. It means we recognized a fraudulent practice and saved the Navy, and the U.S. government money. It also means we ensured that the security and investigative elements cooperated in a timely and effective manner to preclude an opportunity for espionage. And, it also means that our security forces provided not just protection, but deterrence.

You will notice that this edition of *Sentry* is more balanced in its application to all the Navy security disciplines represented by NISCOM. You may be a representative of a smaller community which previously received more attention in past editions of *Sentry*, and may feel that "your" newspaper is being adulterated. Stop and reflect, however, on what I said last issue about the importance of serving all personnel. We are here to complement each other and many of our individual tasks go hand-in-hand with other security aspects. Together, we are a total security concept.

Security starts at the perimeter of the base and ends with a single piece of classified paper or weapons component. Law enforcement resources enforce security requirements. Everyone involved in security, investigations, and law enforcement work within their respective areas of responsibility, but work together in the "big picture."

Let's ensure that you recognize where you fit into the "big picture" and who else is there working with you. You are Security Managers, Top Secret Control Officers, CMS Custodians, Contracting Security Officers, Technical Surveillance Countermeasures Technicians, TEMPEST Control Officers, watchstanders, roving patrols, Masters-at-Arms, Special Agents, ADP Security Managers, NATO Security Officers, dog handlers, personnel in the Nuclear Weapons Personnel Reliability Program (PRP), gate guards, Marine Corps Security Forces, MP's, and also, security-conscious Americans in the Navy or Marine Corps.

Future editions of *Sentry* will continue to be more broadly directed to everyone who works in security or is impacted by security...that is all of us!

Sentry is news, it is guidance, it is kudos, and it is advance notification of policy. Mostly, *Sentry* is a tool for each of us to use to learn or share ideas. Make *Sentry* work! Make it part of the impact I've been talking about. Pass it around. Call special articles to the attention of your shipmates. Post them on bulletin boards. Use them in your daily work. Tell your CO or XO that you want to **"have an impact!"**

And when you've succeeded, when you've had that impact, let us know so we can tell others about it in *Sentry*.

John E. Gordon

Advice from the Detailer

What can you do when 'they' won't let you do your job?

by MACM C. E. Cochran
MA (E-6/E-9) Detailer, NMPC-405C

One of the worst phone calls a detailer can receive from the fleet is the one with a member saying, "Master Chief, I need to transfer because the command won't let me do my job."

My first inkling is to ask, "Who is at fault?"

If you have not proven yourself to be the most professional petty officer or chief petty officer at that command, then something is missing on your part. *(See MA1 Hurley's article next page)*

If, on the other hand, your command has a misconception of the function of today's Master-at-Arms, then we need to educate the command.

No longer are we the biggest and meanest guy on board who is simply expected to hand out linen and monitor the liberty line and chow line. The fact of the matter is we are as technical as any other rating in the Navy when modern police tactics are employed as a daily routine for problem solving.

With the present terrorist threat and political unrest worldwide, each command must be ready, willing and able to respond with swift and decisive action to counter any threat. The only way that can be accomplished is for the command to realize that the Masters-at-Arms on board are professional law enforcement and physical security experts, and each Master-at-Arms must realize that the only way the command will know that is for us to project that professionalism 24 hours a day, seven days a week, both on and off duty. ★

Moving up

Congratulations to the following personnel who were promoted to their present ranks during the latest promotion and advancement cycle.

Lieutenant Commander (6490)

Gerald E. LoPorto

Lieutenant (6490)

Ricky D. Bogle
Steven R. Cole
Jimmie G. Jolliff
Peter J. Mullin
Timothy G. Mueller

Master Chief Masters-at Arms

Orlando B. Cacao
Michael E. Crawford
David B. Durham
Ralph S. Herzog
Laurence M. Hick
Thomas L. Johnson
Michael W. Kohler
Michael Koutroubas
Timothy M. Peckham
Robert P. Rehrig
Robert P. Sailler
Richard K. Spring
Joseph D. Vetro

Senior Chief Masters-at-Arms

Cesar F. Adan
George J. Ball
William A. Bentley
Christopher Berit
Joseph C. Bernardo
Bay Berromilla
James R. Bishop
Ron Blankenship
Charles G. Boggs
David W. Broadway
Donna L. Caddis
Richard P. Chaney
Sue M. Cunningham
Robert D. Fulton
Ronald E. Griswald
Jimmy Hammond
Patricia C. Hix
Larry L. Huddleston
Patricia A. Huntley
Anthony F. Hurban
Romulo F. Ignacio
Jeffrey T. Johnson
Boyd Keele
Albert C. Lawson
David M. Mendoza
Karen D. Parker
Maurice L. Parks
Robert G. Porter
Alan E. Powell
John W. Reid
Donald C. Roberts
Jesus Rodriguez
Robert R. Ruger
Ladonna R. Selby
Thomas G. Sidel
Mark H. Siebert
Gordon F. Starr
Janice L. Svec
Ronald L. Wiebe
Robert L. Wimbley
Billy J. Woodruff
Randolph L. Wright

Chief Masters-at-Arms

Gerald Anagnostou	Mark Anderson	Lawrence G. Baginski	Robert L Baldwin
Emilio Balmaceda	Francisco L. Batac	Richard C. Berry	John J. Bicknell
Melvin P. Brege	John Cavanaugh	Robert L. Chaney	Leonard Chapman
Francis C. Cherry	Steven F. Childs	Etsel V. Cole	Charles Compeau
Louis S. Conway	Bonnie K. Criswell	Walter K. Croxton	Glenn P. Davis
Matthew W. Davis	Frederick R. Diehl	Patricia L. Duwel	Vaughn M. Ehrman
Jerry A. Eicker	Jeffrey T. Elkins	Gerry S. Feild	Daniel Ferris
Edward P. Fulk	Richard Furmaniuk	Robert L. Goldfinger	Paul R. Hahn
Paul A. Hardesty	Mark W. Hardin	Jenilee K. Harris	Miles J. Harvey
James M. Head	Robert D. Herbert	Anthony Hernandez	Robert K. Hill
Linda C. Horne	Brian D. Jacobson	Raymond S. Jahnke	Thomas G. Jessen
Larry R. Jones	Frederick Kalmbach	Steven R. Kinder	Lance Kleinsmith
Phillip S. Lafrance	Charles J. Little	Eddie J. Lyons	Robert Maldonado
Edwin C. Mateo	Archie C. McArthur	Sara G. Miller	Cheryle L. Mills
William Moriarity	Hans M. Nagorr	Everett E. Newsome	Bobby W. Ozley
Rodolfo H. Pangan	Taresa L. Phillips	William A. Pitard	Tony A. Ramey
Eduardo Ramirez	Ellen K. Ramsey	Jerry D. Ranger	Wayne A. Reay
Herman J. Redding	Jacquelyn Rochelle	Robert A. Rook	Mary A. Seymour
James Siegel	Michael R. Smith	William H. Spangler	Mike L. Springsteen
Frank G. Stoeffler	Robert G. Stover	Billy R. Stroups	Ronald Suggs
Steven A. Szalo	Stephen D. Thomas	Jon P. Thompson	Ronnie L. Turnbull
Dale E. Tuttle	Robert J. Utter	Adalberto Vasquez	Russell H. Wagner
Jacquelyn D. Webb	Elisabeth J. Weier	George A. Willis	Mercedes Wilson
Daniel T. Wright	Christine L. Zunkel		

First Class Masters-at-Arms (SEP 88 Cycle)

Kenneth T. Aanensen	Anthony M. Allen	Michael Anders	Patricia L. Appleton
Kathleen Avery	Richard J. Banks	Donna Baptiste	Nancy K. Bobo
Ronald Bouldin	Quinton E. Brown	Eric J. Collins	Michael W. Conn
Cathy L. Cooksey	Catherine L. Drezak	Clyde W. Dunaway	Cheryl Etherton
Betty Feeley	William A. Fenby	Debra A. Flynn	Gerald P. Gioavgnoli
Bruce O. Girkin	Edward C. Golmond	Tracy A. Gonzo	James W. Harrington
Richard Hayman	Hugh B. Hermitage	Richard A. Hewitt	Denise Hill
Richard A. Kerckhove	Eric L. Lashley	Brian W. Lawn	Kenneth Lazorchak
Shannon Lovejoy	Christian MacHidon	Vincent S. Malgioglio	Dorrise J. Maxwell
Ronald Mayfield	Mark McCready	Arthur B. Mead	Pamela Medearis
Glen E. Mendenhall	Timothy H. Moes	James W. Moon	Gary S. Morgan
Michael Newell	Jeffrey A. Nickerson	Louie J. Osborn	Pauli Pickering
Donald K. Powell	Victor W. Quiroga	Larry H. Ramos	Eugene Richley
Jaime R. Rodriguez	Victor R. Rule	Walter P. Schmid	Jeuel F. Seal
James R. Searles	John D. Segrest	Jerry M. Singer	Edward M. Stack
Mark D. Sterling	Anthony R. Stewart	Pamela A. Stout	Debbie S. Tamlin
Kenneth Thompkins	Renato Tiongco	Gregory A. Trumbull	Karen L. West
Edward Whittington	Theodore Young		

Advice from the Rating Advisor

Overcoming the Stereotype

by MA1 Thil D. Hurley
Former NISCOM Asst. for MA Programs

Since the Navy was established over 200 years ago, many changes have taken place. The Master-at-Arms (MA) originally was a senior petty officer aboard a sailing ship who was responsible for the safeguarding and issuing of firearms and weapons.

As the Navy matured, the role of the MA expanded to include the enforcement of Naval law, maintenance of berthing spaces, and general crew welfare. With the reduced emphasis of crew's marksmanship, the MA's role began to be overlooked and the position evolved into one of simply handling linen and supervising chow lines. Of course, the individual assigned to this job was normally someone not greatly needed elsewhere, and as a result, MAs soon became stereotyped as "less than average sailors" who were MAs only because they did not perform well in their own ratings.

In 1973, the Master-at-Arms rating was established as a separate entity in response to an increased need for trained law enforcement and physical security specialists. Today the MA is as completely different from his sailing-ship ancestors as man is from his Neanderthal counterparts.

Unlike the MA of old, applicants must now meet stringent selection criteria and be evaluated as top-performers in their field. Formal law enforcement training is demanding, both physically and mentally, and promises to remain tough.

In today's environment, the job of

(Continued on following page)

STEREOTYPE

(Continued from previous page)

an MA has become everything but low priority.

Since OP-09N assumed rating sponsorship of MA's in October 1986, the "new" MA is trained to work closely with NIS agents involved in drug interdiction efforts and felony investigations, as well as the routine duties aboard ship and shore stations.

To further enhance the professionalism of the rating, guidelines have been developed to ensure that appropriate quality controls are maintained on MAs in the fleet. They must maintain impeccable service records after conversion. MAs not performing up to standards will be removed from the program and reverted back to their former rating. This ensures continuance of the high standards necessary to provide the fleet with trained law enforcement professionals.

Today's Master-at-Arms -- professional law enforcement and physical security. MAC John F. Phillips, NAF Washington DC, processes a crime scene. (Photo by JO1 John S. Verrico, NISCOM)

Unfortunately, some people still characterize today's MAs as insignificant. Because of this, some MAs may have to start at the ground floor in obtaining the professional respect of their commanding officers. This professional trust and reliability is absolutely essential for MAs to do their job correctly, and it is up to each MA to change this damaging image of the rating.

If you are trying to improve rapport with your command, there are some things you need to keep in mind.

The attitude with which you approach a situation is 90% of the battle and as a senior petty officer it is your responsibility to obey your chain of command, even if it does not function like you think it should. There is some truth to the axiom that "the squeaky wheel gets the grease," but the old saying that you "can catch more flies with honey than vinegar" often works better! Butting heads with your senior officers is not the best interpersonal communication skill to use.

Instead of confrontational tactics, try proving your professionalism and reliability through the superior performance of whatever tasks you're assigned. Expand your responsibilities by requesting collateral duties in areas that you want to improve, and make those areas better. Don't lose patience due to slow progress since it may take time to establish credibility. Remember that each accomplishment that you achieve will cause that command to take notice and will build that all-important professional trust.

Another aspect of professionalism is the desire to continue your training and development. Just because your command does not fully support your training program does not mean that your professional growth has to stop. Take advantage of the opportunities available to you to continue your training during off-duty time through affiliations with professional groups, local law enforcement agencies, and civic organizations. Becoming involved in reserve police units, fire or rescue departments, or even Little League baseball teams, displays your desire to develop professional and leadership skills through community service.

In addition to efforts in the local community, there are innumerable law enforcement related correspondence course from all branches of the service that can enhance your job performance and knowledge. Opportunities for technical or college-level education should be taken advantage of as well.

Remember, the only person who can stop your professional growth is you.

Through dedication to service and continued development, both personal and professional, your value to the command will become evident and you will begin to see the improvements in attitudes, which will make your job more satisfying and rewarding. Through your leadership example, you can change the image of today's MA force. Even if you never reach your ultimate goals, your efforts will greatly benefit your relief, who won't have to start at the bottom all over again. **Think positively! There are no *problems* -- only *solutions*!** ★

Manpower shortage in MA rating

by MA1 Thil D. Hurley
Former NISCOM Asst. for MA Programs

The results of the recent selection board pointed out a concern that needs to be redressed -- applicant recruiting.

The Master-at-Arms (MA) rating is currently manned at only 76% overall and the fleet continues to be in desperate need of MAs, especially Second Class Petty Officers and Third Class eligible for advancement. For the past few years, the rating has been one of only a few allowed to increase its manpower end-strength. This was permitted in order to meet the Navy's requirements for professional law enforcement and physical security personnel.

But the trend is in jeopardy of changing -- for the worse. The MA community, like many other ratings, is trying to maintain its growth due to our ever-increasing commitments worldwide, but applications for conversion to the rating have been declining. This means that we can not even fill current billets, much less those projected for the near future. Because of an inability to fill billets, some billet cuts are already scheduled. If this trend continues, the MA rating maybe forced to make additional cuts which reduce your chances of having a trained MA partner and could adversely impact future promotional opportunities.

In order for the MA community to continue to meet its expanding responsibilities, we need to convert many more applicants than we are doing now; however, the high standards that have been established for the rating *cannot* be lowered.

This need is very clear. MAs in the fleet need to make recruiting prospective applicants a high-priority in their day-to-day contacts. Career counselors are being made aware of the need and are becoming helpful, but the major emphasis is placed on MAs in the fleet to seek out ***qualified*** candidates and help them achieve a career in the Master-at-Arms community. Being a "recruiter" may sound unappealing to some of you, but it is essential for the well-being of the rating and it's easier than you may think.

How many times have you run across a shipmate who appeared interested in what you do? There's a prospective candidate right there! Now all you have to do is make sure that they are up to the standards required of an MA, provide them with a good background in preparation for conversion, and assist them with their application package.

Don't be concerned about becoming an expert on the conversion process -- that's our job and you can contact us with any questions. Most importantly, don't let anyone tell a prospective candidate that they can't convert until you've checked it out. A lot of prospective candidates failed to apply because they were misled about requirements -- that's a mistake that shouldn't happen to anyone.

As rated MAs, we have an interest in seeing that only qualified candidates become MA selectees. Our rating is at a critical point in its development and everyone needs to make their best effort to support its continued growth and professionalism. We can't afford to lose the progress we've made.

MA Conversion Board (October 1988) Results

Congratulations to the following individuals who were selected for conversion to the Master-at-Arms rating by the October 1988 Selection Board.

Charles Abron	Mark Anderson	Mary K. Barney	Robert J. Benson
Austin L. Bentley	Jimmie W. Brown	Robert A. Burgett	James W. Cain
Joseph L. Casey	Kenneth Davenport	Frank W. Davis	Wayne M. Demoga
James W. Dennison	Dorinda K. Dodd	Steven C. Doire	Jon E. Doliana
George P. Doyle	Richard M. Eaton	Jimmy E. Elam	Mark A. Emerson
Joseph D. Felker	Steven C. Flynn	Eugene D. Foss	C. F. Franceschini
Brian Gibbons	Kathy D. Goetz	Roger L. Hilliard	Daniel A. Hines
Daniel Kiliszewski	Kevin K. Klar	Gerald C. Laverty	Kieth L. Lowe
Reginald D. Madison	Thomas E. Miller	Sandra J. Moore	Todd G. Mutchler
Joseph A. Paradise	Jeffery T. Parron	Clifford W. Partin	Thomas H. Poston
Gary L. Prebyl	Thomas Reichenbach	Jacqueline Santillanes	Jim Schellenberger
Barbara A. Schmees	Raymond Simoneau	Steven Smalkowski	Mark J. Smith
Joseph R. Stratton	Otis S. Sutherland	Vat L. Thompson	Kenneth Trantham
Halekila Tuipelehake	Paula J. Uecker	Richard T. Voss	Robert Wadsworth
Carol A. Wedeman	Kerry D. Weeks	Jeffery T. Wright	

Navy's largest shipyard offers unique police duty

by James J. Reaves, Chief of Police,
DoD Police, Philadelphia Naval Base

In 1775 the Continental Congress, meeting in Philadelphia, Pennsylvania, provided for the outfitting of two small wooden sailing vessels to protect our coasts. That work was also done in Philadelphia, and ever since, the city has played an active role in the U.S. Navy.

The nation's first naval shipyard was established in Philadelphia in 1801 on an ll-acre tract purchased from the city for $1.00. With the advent of the iron-clad ships during the Civil War, it became apparent that the shipyard needed more space, and in 1865 it moved to its present location about three miles south.

Now situated on more than 2000 acres within the city's southern-most boundaries, Philadelphia Naval Base is, in actuality, a small city within the city. More than 7,000 military personnel and their dependents live in the base's residential district while an estimated 17,000 vehicles enter the base's business and industrial areas each day, bringing the workday population to over 50,000. Within the 10-mile perimeter are 52 miles of street and 4.5 miles of busy waterfront.

The Philadelphia Naval Shipyard is the Delaware Valley's largest industrial employer with more than 9,000 civilian workers, five drydocks, and over 1300 buildings offering more than 7 million square feet of shop space. The Shipyard is also the largest of the 36 separate naval commands aboard the Naval Base. Other major activities include the 226-prisoner Naval Brig (second largest of all service brigs in the nation); the Inactive Ships Detachment, which maintains a 'mothball fleet" of WWII and Korean War ships; the Naval Damage Control Center for shipboard firefighting training; and the nation's largest Naval Reserve Center complete with the largest fleet of Naval Reserve ships.

Over the years the shipyard has built 125 ships, everything from wooden sailing vessels to the battleships New Jersey and Wisconsin. In the early 1970's its mission was changed to overhauling, refitting, and converting the Navy's conventionally powered warships. Currently, it specializes in overhauling sophisticated surface ships and aircraft carriers.

Now the bulk of the yard's workload is the highly complex Service Life Extension Program, which by rebuilding aircraft carriers, can stretch limited tax dollars by extending the life of each carrier a minimum of 50% for about 25% of the cost of a new one.

With this much going on, the area poses some unique law enforcement and security problems.

The Department of Defense (DOD) Police Department uses a combination of civilian DOD police officers and Master-At-Arms to provide police protection for the entire base complex. At 150 strong, it's one of the largest DOD Police Departments in the nation, and in scope and size ranks as the 17th largest of 1326 Police Departments in Pennsylvania.

The department which is broken down into three divisions: Patrol, Special Patrols and Administrative Support.

Routine police protection is provided around the clock by the Patrol Division, handling most of the 200 daily police calls, which range from parking tickets (over 1100 per month) and moving violations (over 300 per month), to major accidents and serious crimes.

A special security problem is posed by the base's 4.5 mile waterfront and a number of warships sitting in drydock or at pierside, which are completely vulnerable. The answer to the problem is a 15-member Marine Unit, part of the Special Patrols Division, that patrols the waterfront 24 hours a day in maintaining a 100-foot security zone around the ships and piers. The unit also provides assistance to the Philadelphia Police Ma-

Used by the Tactical Unit for weapons and equipment transport, the Emergency Services Unit is equipped with a star-scope which enables police to see in the dark (Photo by Ptlm. Jerry Welsh)

rine Unit and the Gloucester City, N.J. Coast Guard Unit. Working out of a 33-foot steel-hull police boat (equipped with radio, flood lights, and fire fighting equipment) the unit has assisted in waterborne emergencies such as shipboard fires, explosions, and pleasure craft rescues.

An Accident Investigation Unit handles all vehicle accidents, completing and filing the Pennsylvania Police Accident Report for more than 700 reportable accidents each year, and operating radar to ensure compliance with the speed limit.

Another Special Patrol unit is the K-9 Unit. Using two "explosive dogs", two narcotics dogs and two patrol/tracking dogs, this unit performs searches for controlled substances, responds to all bomb threats, and provides additional security for visiting dignitaries. The team is frequently dispatched throughout the Northeastern United States to assist in bomb and narcotic searches and special operations, such as Philadelphia's "We-The-People 200" celebration, the President's visit to Dover Air Force Base, the Pope's visit to Texas, and the Pan American games in Indianapolis.

Tasked to respond to the increase in terrorist activities around the world and an increase in serious crime at the Naval Base, the department has formed a Tactical Operations Unit (or SWAT team). This unit of the Special Patrols Division performs when additional security is needed, such as protective service details for visiting VIPs, security for Army-Navy Game Day and ship arrivals or departures. Members receive extensive training from a variety of federal, state and military tactical operations teams, as well as continuous in-service training on all aspects of special tactical operations. As part of its regular training, and as a community service, the unit sponsors a semi-annual Police Combat Tactical Pistol Match at the Naval Base which is open to and attended by over 100 area police officers as well as DOD officers.

Philadelphia's Mobile Communication and Command Post bus is equipped with a 12-person conference center and a communication room with police, fire, ambulance, military, shipboard and aircraft radio equipment, cellular telephones and two roof-mounted high-powered video cameras for viewing and recording accident and disaster scenes. (Photo by John Long)

The Administrative Support Division controls the Armory, which maintains the department's 212 weapons; the Tow Squad, which retrieves over 50 abandoned and recovered stolen vehicles per month; the Crime Prevention Unit, which presents 16 different crime prevention programs each year to base residents; Communications, and the Automotive Services Unit, which maintains the fleet of 23 vehicles including police patrol cars, paddy wagons, mobile communication/command post, tactical unit, and motorcycles.

In today's "bottom-line" conscious society, one of the more difficult tasks facing any police department is tying everything together into a meaningful report that accurately reflects the department's activity. That task falls upon the Crime Analysis Unit. The unit identifies and plots crime trends through computer analysis of all police and investigative reports and also produces a monthly management summary that measures the productivity of each officer, platoon, and special patrol unit.

The members of the DoD Police Department at Philadelphia are proud of their accomplishments. A deep sense of responsibility to provide professional police services to the community, and a dedication to maintaining high standards, have helped them develop into one of the most progressive police departments in the Navy. ★

contains timely and informative articles concerning crime prevention efforts. Every security department in the Navy should be on the mailing list of NCPC. Their address is **National Crime Prevention Council, 733 15th Street N.W., Washington, DC 20005.** The phone number is **(202) 393-7141.**

AMERICAN ASSOCIATION OF RETIRED PERSONS (AARP) -- Primarily organized to represent the interests of retired persons and the elderly, the AARP actively promotes crime prevention programs to reduce opportunities for their victimization by con artists and others. Their awareness programs are equally as informative to the general population as to their target groups and the AARP produces excellent material. Camera ready prints for photocopying, pamphlets, films, video tapes and other information can be obtained from them on a loan basis, for free or, in some instances, at a nominal fee. For information, write to: **American Association of Retired Persons, 1909 K Street N.W., Washington, DC 20049** or call **(202) 728-4363.**

NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN -- The National Center for Missing and Exploited Children is a national clearinghouse for information collection, storage and dissemination regarding missing or exploited children. Under grants from the Department of Justice, they have published numerous pamphlets entitled *JUST IN CASE...*, dealing with missing, abused and exploited children. Additionally they publish information pamphlets on runaways, dealing with grief over the loss of a child, parental kidnappings and an assortment of other timely and important topics. Every law enforcement agency in the United States, including every Navy security department, should be aware of the Center's offerings and no crime prevention coordinator should be without copies of their material. The address is: **National Center for Missing and Exploited Children, 1835 K Street, N.W., Suite 700, Washington, DC 20006.** Their information telephone number is **(202) 634-9821** and they have a toll-free hotline for information that could lead to the location and recovery of a missing child, **1-800-843-5678.**

OTHER RESOURCES -- Crime prevention is a bonding agent between all segments of society. Crime on a Navy installation affects the surrounding civilian community and vice versa. Civilian law enforcement agencies, for the most part, have dedicated programs that they will share with your department. Additionally, local community groups, state sponsored programs, private industry, professional organizations, service clubs and other organizations can assist you through volunteer efforts or through crime prevention materials that they will donate to your program. Soliciting funds from sources outside the Navy is expressly forbidden by law and regulation. If, for instance, a service group such as the Lions International, a Rotary Club or even one of the wives clubs on base wanted to give your department money for crime prevention, you cannot accept it. Many clubs do fund the printing of crime prevention booklets and will donate them, as a service project, to law enforcement departments. Check with the base legal officer for guidance on these matters.

To meet the needs of your department's crime prevention program, more than anything else, the coordinator must be enthusiastic and dynamic in delivery of this service. For this reason, the coordinator should be a self-starter, reliable, experienced in law enforcement and have a track record as one of the hardest working members of the organization. Building your program around such a person guarantees success. ★

Awards available for crime prevention efforts

by Carlton A. King
NISCOM Administrative Assistant for Crime Prevention Programs

The Crime Prevention Coalition, composed of over 120 member organizations, including the U. S. Navy, recognizes outstanding crime prevention initiatives during its Annual Awards Program. Selectees in each category are flown to Washington, DC to be honored at an awards banquet. This year there were almost 100 nominations submitted to the Awards Committee on which I was priviliged to be a member.

Nomination packets had been sent to most major claimants and to nearly 100 Naval activities identified as having crime prevention programs. Unfortunately none of these Navy nominations were submitted. Through daily telephone conversations with chiefs of police, security officers and crime prevention coordinators throughout the Navy, it is apparent that we have an abundance of dedicated people and effective programs in the field that would have qualified to receive a national award. Hopefully, next year's awards committee will have several nominations from Naval activities so that those who work hard to prevent crime can be recognized for their efforts and their successes can be shared with others.

Sitting on the judging panel was an educational experience. Should your security department elect to submit nominations for the 1989 selection process, the following advice might benefit you in the preparation of the nomination packet.

FOLLOW THE INSTRUCTIONS

This warning is as important as those in the last issue of *Sentry*, where two articles (one dealing with the selection process for LDO/CWO and the other with Master-at-Arms conversion) highlighted the importance of neatness and completeness when submitting packages for consideration. If, for instance, an instruction or application requires three reference letters, submit three and don't try to bolster your application by submitting five or try to abbreviate the process by submitting two.

FOLLOW THE FORMAT

Enclosures or attachments should be arranged in ***precisely*** the order required by the application. During the screening process an initial review is conducted to verify the eligibility of nominees and to ensure that packages conform to published requirements. This is prior to the formal review for awards determination. Your application, regardless of content and quality, may be discarded for "**Failure to follow directions.**" Again, this advice is similar to that given in the above referenced *Sentry* articles.

PROMOTE ONLY THE PERSON OR PROGRAM NOMINATED

Your narrative is limited to a set number of pages or words. Use this space wisely by directing the reviewer's attention to the person or program being nominated. Several of the packages we reviewed spent more time promoting the department or the company than the key person or the program they were nominating. Remember, bigger is not necessarily better, especially considering that the panel has many applications to go through and limited time to review packages, which is why restrictions are placed on the number of pages or words in the first place. Unnecessary information detracts from more important material and blurs the vision of reviewers when considering the totality of the nomination.

BE HONEST

Awards are generally not granted for routine performance. Do not submit a nomination if your only motive is to boost the morale of a person or program. Competition for these awards is stiff and ordinary performance will not be sufficient for an award. Instead, ask the following questions: What was done above and beyond that which is required? One nominee considered by the recent Awards Committee is a deputy sheriff assigned to patrol duties with collateral duty as a crime prevention officer. In the course of a year, he worked more hours on crime prevention programs ***off duty*** than hours worked for salary. When the new budget allowed for him to be compensated for some of his accumulated overtime hours, he requested that the money go toward purchase of crime prevention material rather than personal reimbursement. Without question this is an exceptional example, but it illustrates a situation where a nominee exceeded the norm.

INNOVATION AND CREATIVITY

In the selection process, nominees who either tailored established programs to meet unique needs, or created new programs, were given a lot of consideration for their efforts. This trait could be excellent justification for an award. What, for instance, has a Master-at-Arms done to reduce thefts aboard his vessel? How has the reported theft rate declined as a result of the effort? How much money was saved? How can the program be implemented aboard other ships?

STATISTICAL DATA

Whenever possible, nominations should include a summary of statistical or numerical data. Information such as population of the activity, crime comparisons between specified time periods, hours spent in crime prevention efforts and anything else that quantifies the program effort will help in the decision process.

The quality of crime prevention in the Navy is rapidly increasing. One main element of professionalism is recognition for contributions toward the improvement or enhancement of the career field. Therefore, it is important that supervisors take advantage of the benefits derived from awards programs of this nature and nominate people deserving of recognition, such as crime prevention coordinators, block captains, OMBUDSMEN or others who contribute to making the Navy a safe and crime-free community. ★

Two Navy commands receive awards for National Night Out programs

by Carlton A. King, NISCOM Administrative Assistant for Crime Prevention Programs

The National Association of Town Watch, Inc. (NATW), a non-profit membership organization dedicated to the development and promotion of organized crime prevention operations, recently recognized two Navy activities for their contributions to, and participation in, the 1988 National Night Out campaign. Of the five military awards given this year, two were received by Navy installations. This is indicative of the progress that Navy security departments are making in the field of crime prevention.

On 9 August 1988, over 18.5 million people in over 7,000 communities participated in National Night Out. Concerned citizens, business groups and law enforcement departments participated in a joint effort to ensure a crime-free night by keeping porch and patio lights on, hosting block parties and working together to convey the message that neither crime nor criminals would be tolerated in their neighborhoods.

Naval Air Station Memphis, Tennessee was one of the national award winners. The Chief of Police at NAS Memphis, Master Chief Master-at-Arms Charles R. Kellogg, related that a tent had been set up behind the security department in which there were various displays of home security devices. The security department provided a visit by McGruff, the Crime Dog; served snacks; and sponsored a crime-free evening for NAS Memphis personnel and their families. Crediting Chief Master-at-Arms Sidney Bonhomme with a dynamic and dedicated effort to promote crime prevention and safety, Kellogg estimated that between 75 and 100 participants joined with the security department to celebrate National Night Out.

The other Navy recipient was Naval Weapons Station Charleston, South Carolina. Chief of Police Steve Gagat and Crime Prevention Specialist Sgt. Linda Sumey made a special effort to "turn on the lights and turn off criminals." In two separate housing areas of 20,000 and 5,000 personnel, Gagat and Sumey organized parades and attended approximately 35 block parties celebrating National Night Out. As a symbolic gesture, base residents joined hands while standing outside their homes. This, in effect, established a "shield of neighbors" unified to support one another in an effort to rid their community of crime. Gagat and Sumey credit their success to the support they received from the Commanding Officer, Executive Officer, OMBUDSMEN and Block Captains who were instrumental in the organization and logistics efforts. Sumey said, as with previous National Night Out programs, there were no reported crimes that night. ★

National Night Out will take place next on 8 August 1989. If your department would like to participate, contact the National Association of Town Watch, Inc., P.O. Box 303, Wynnewood, Pennsylvania 19096.

Looking for '1H'

by R. R. Gorena, Deputy Assistant Director,
NISCOM Information and Personnel Security

"Have you seen the new Navy Security Manual, you know, OPNAVINST 5510.1H? What, you have 40 copies? It's dated 29 April 1988! Well, I don't have mine, nor do other commands on this base. How do I get copies?"

How many times has this conversation taken place in the last few months? Why didn't everyone get their new security manuals even though they are on the Standard Navy Distribution List (SNDL), Parts 1 and 2, or on Marine Corps Distribution Code DL? How do we get our desperately needed manuals?

Distribution of OPNAVIST 5510.1H has been completed. That's what the Naval Publications and Forms Center (NAVPUBFORMCEN) claims and all ships and stations should have received their copies.

So, what happened to them?

The Naval Investigative Service Command (NISCOM) Information and Personnel Security Directorate looked into the matter and sought to trace distribution. They found that in some cases, distribution copies were received by the command, but were retained by other offices, rather than being routed to the Security Manager. Some copies were rejected and shipped back. In other cases, they may still be in supply centers or mail rooms in cartons.

Distribution was made according to the SNDL. The copies are "loose leaf, three hole punched, clear plastic-wrapped, and 1 1/2 inches thick." Multiple copies were shipped in corregated cartons of 12 each and were addressed to individual commands.

All Security Managers should check with their supply clerks, mail rooms, or loading docks to ensure that their 1H's aren't sitting there, unrecognized. When all these channels have been exhausted, order copies directly from the NAVPUBFORMCEN -- don't call OP-09N as no stock is maintained in Washington.

Change ONE to OPNAVINST 5510.1H is ready to go to the printer.

There are many security policy matters in "1H" and Change ONE, BOTH of which require Security Manager and Command attention. Don't wait any longer for the 1H to get to you. Make a local survey, then take steps to get NAVPUBFORMCEN to send you a copy. ★

Naval Publications and Forms Center

Mailing Address:
Commanding Officer
Naval Publications and Forms Center
5801 Tabor Avenue
Philadelphia, PA 19120-5099

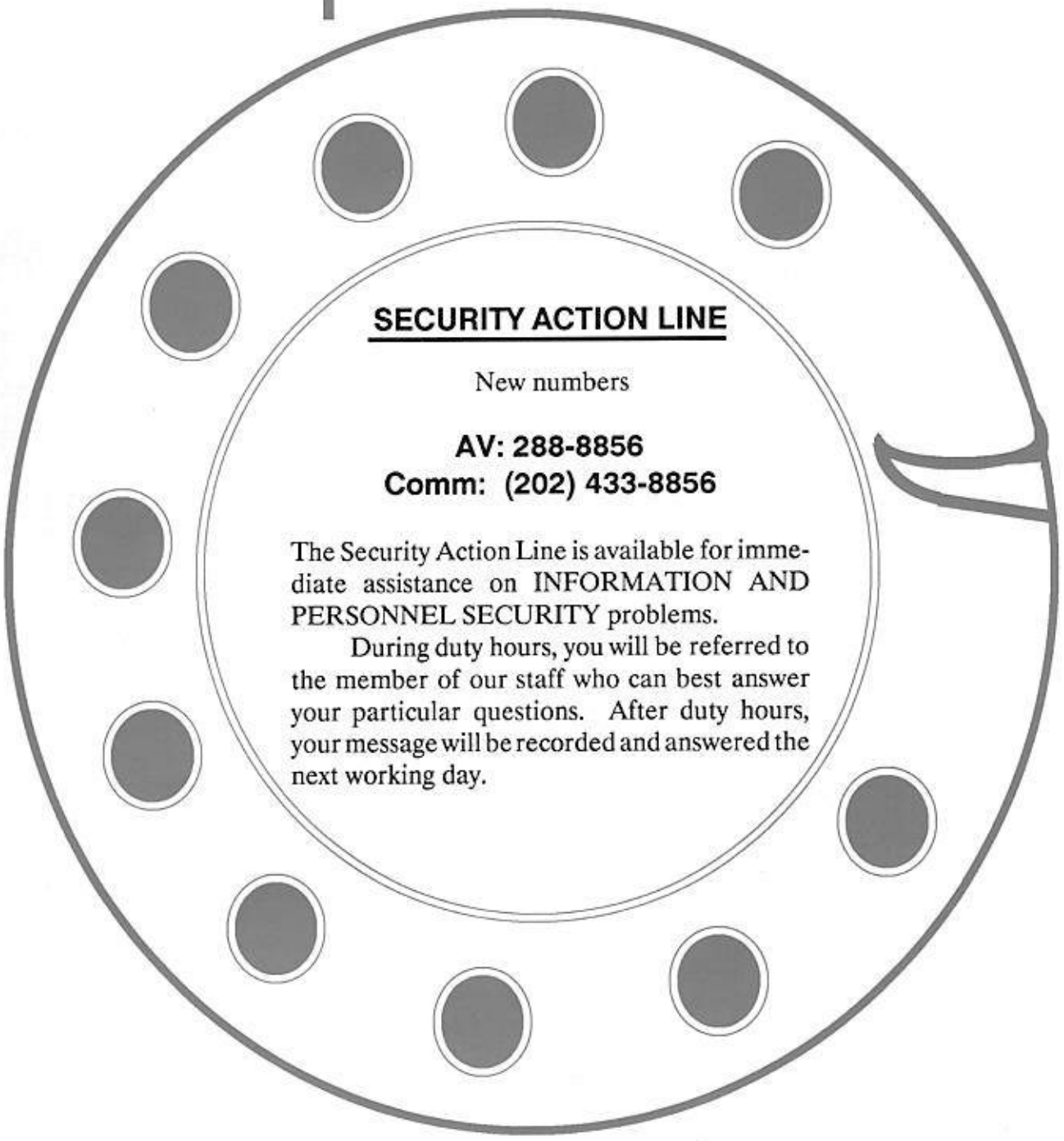
Unit Identification Code (UIC): N00288
Routing Identifier: NFZ

TELEX Number: 834295
Western Union Number: (710) 670-1685
Telecopier: Autovon: 442-5912
Comm: (215) 697-5914

Customer Service Phone Numbers:
– Specifications/Standards Requisitioning (Emergency orders only - limited to five (5) line items)
Autovon: 442-3321 **Comm: (215) 697-3321**

Message Address: NAVPUBFORMCEN PHILADELPHIA PA
Hours of Operation: Mon - Fri, 0800 to 1630 EST. Refer to NAVSUPPUB 2002 prior to ordering.

New phone number



SECURITY ACTION LINE

New numbers

AV: 288-8856
Comm: (202) 433-8856

The Security Action Line is available for immediate assistance on INFORMATION AND PERSONNEL SECURITY problems.

During duty hours, you will be referred to the member of our staff who can best answer your particular questions. After duty hours, your message will be recorded and answered the next working day.

Same 3 security infractions top the list...again!

Each year, the Information Security Oversight Office (ISOO) issues a report to the President on how the Agencies of the Executive Branch are managing information security. We provide detailed statistics from the Department of the Navy.

Again last year, the **same three** security infractions appeared at top of the list:

Mismarking -- over 50%
Improper storage -- nearly 28%
Unauthorized transmission -- over 11%

Look at your information security program. How do you stack up against these national statistics? ★

Original or derivative?!

by R. R. Gorena, Deputy Assistant Director
NISCOM Information and Personnel Security

The headline carries both a question mark and an exclamation point. It could also carry other symbols, such as #@&*$?! Why, because the words Original versus Derivative, in the context of security classification, cause many people to rack their brains trying to determine exactly what or who is *the* classification authority for Department of the Navy classified information.

Let's start with a good source of informatiom. Chapter 6 of OPNAVINST 5510.1H is an excellent "primer" on classification. Every person who applies a classification to Navy or Marine Corps information should be fully conversant with this chapter. Strict rules must be followed each time a classification is applied. Make sure you consult Chapter 6 and you won't go wrong.

And, what about downgrading and declassification? The same chapter applies; particularly Article 6-6.

Who is an Original Classification Authority, you ask? Exhibit 6A lists the ONLY officials in the Department of the Navy who may classify original information. There are 107 TOP SECRET and 353 SECRET Original Classification Authorities. CONFIDENTIAL classification authorities are not specifically designated.

These are the people who designate the original classification, but over 90% of all classification markings are "Derivative!" Anytime you use someone elses classification, in word, phrase, sentence, line, paragraph, etc, you are deriving your classification from theirs. Therefore: "Derivative."

The Department of the Navy has Classification Guides for almost every program, weapon system, plan, operation, or platform. The OPNAVINST 5513 Series provides derivative classification to minute details.

Every year, the Information Security Oversight Office (ISOO) requires statistics on how we are classifying information. You may have been tasked to complete the data report which the ISOO uses to compile its report to the President on how we're doing in our mandated efforts to classify properly, and that means, knowing how to classify and not overclassify.

This is where over 50% of the security infractions in the Navy occur. If we all understand how to classify, imagine how we can SIGNIFICANTLY reduce the infractions in the Navy and Marine Corps -- BY HALF! ★

FADE TO BLACK...

"Trash Ops" in the Philippines

by S/A Richard J. Sullivan
NISCOM Damage Assessment Branch

FADE THEME MUSIC, FADE IN -- *A soaring Philippine Eagle lazily rides the on-shore breeze, searching for a morsel of food amidst the quickly drying road-kill on the "Zig-zag" National Highway far below. Barely two hours past dawn, the bright tropical sun flares into the camera's view over the tops of the swaying coconut palms on a nearby hilltop as it coaxes the dry temperature into the high nineties.*

SLOW ZOOM -- *Three Filipino scavengers, who, wearing only cut-off blue jeans, soiled T-shirts, worn shower shoes and the eternal air of the optimist, are working the landfill site at the U.S. Naval Station, Subic Bay, R.P. These scavengers, known as "dumpster divers," pick their way through the mountain of fresh morning garbage just delivered by a driver from Alava Pier. As we watch them sort the accumulated and soggy daily debris of fleet operations, one of the three comes across a wad of papers with familiar markings. The papers are in the unclassified trash, mixed in with old Plans-of-the-Day, Navy Exchange and AAFES promotional fliers touting yesterday's sales, last week's Pacific Stars & Stripes newspaper, and an unspeakably smelly combination of coffee grounds, broken plastic, twisted wire harnesses, spoiled eggs, used grits, aircraft parts, and rancid cooking grease. Carefully separating the papers from the other valuable recyclable goods, the men discover an over-stamp with the English word "**SECRET**" on the top and bottom of each page. They carefully pass the papers to their "boss," a time-worn and weather-beaten caucasian.*

He is a silent, private man who could pass for Crocodile Dundee's best friend. He's Hollywood's idea of the "Bamboo American," who scrapes out a living balancing between two cultures in this tropical island nation. He has been doing this furtive work for over a dozen years, always on the lookout for the classified document or the aircraft part or tool which in the "dynamic" economy of Olongapo City translates to quick and easy cash. He recognizes the forms as classified U.S. Naval Messages, containing perhaps the schedules of Seventh Fleet submarines, or amphibious task force ships. This is the fifth package of classified material his scavengers have "recovered" this week, and it's still only Tuesday morning. He is pleased and knows that his "case officer" will also be pleased, not just with the documents, but with the nineteen hundred dollars worth of thermocouples he has stashed in the bed of his beat-up pickup truck. Deciding that it is time to "get rid of the evidence," he smiles to himself as he drives off to meet his case officer.... ***FADE IN THEME MUSIC, SLOW FADE TO BLACK.***

Sound like a spy movie? Well, it's not. It's a real-life occurrence! Does this mean that a bunch of classified information was just turned over to some foreign government? It could -- but not in this particular case. NIS and the Commander, U.S. Naval Forces Philippines, with the support of CINCPACFLT, have been doing something about this hemorrage of classified information. It's a trash recovery operation designed to salvage "lost" government property from the trash at the sprawling U.S. Facility in Subic Bay, Philippines. The operation has recovered thousands of classified documents over the past 15 years. Local Filipinos, who are illiterate in English, are enrolled and trained to search the **UNCLASSIFIED** trash at the dump and recover classified documents which Navy personnel improperly disposed of in the garbage. When they find a document with appropriate markings, they turn it over to an American citizen -- a full-time NIS civilian employee who has been working the "Trash Op" since its inception (and who does indeed look like he'd be at home with Paul Hogan's popular bushman character). He supervises the scavengers and brings their treasures to NISRA Subic Bay. The responsible commands are identified and contacted, and COMUSNAVPHIL and CINCPACFLT are apprised. By now this program is no secret. Incoming ships are warned of the operation. Nevertheless, most visiting ships and local commands have been "hit." Perhaps this accounts for the rumor that some skippers have banned the off-loading of trash in Subic.★

Unclassified but *sensitive*

by Christina Bromwell
Head, NISCOM Security Review Branch

In 1985, Navy commands became responsible for implementing a new program which limited distribution of **unclassified** technical data with military or space application subject to export control. Only "individuals and enterprises that are determined to be qualified U.S. contractors...request[ing] the data for a legitimate business purpose..." may receive such information.

Certification occurs when an individual or firm wishing to participate fills out a DD Form 2345 and submits it to the Defense Logistics Services Center (DLSC) for approval. The form is a contract between the Department of Defense and the submitter which states that the applicant is a U.S. citizen, that he requires certain export-controlled technical data in pursuit of a legitimate business purpose, and that the data will only be conveyed to other certified contractors and will not be exported without a license.

After checking to see if the requestor is on the debarred bidders list, and/or if the person or company has had any export control violations, DLSC approves the form and the enterprise can receive the unclassified technical data.

In 1986, the program was expanded to include Canadian contractors.

'Unclassified technical data with military or space implications cannot be released, except to qualified U.S. contractors for legitimate business purposes.'

Originators must identify technical documents containing export-controlled, militarily critical technology and mark them with the appropriate distribution limitation statement and "notice of export control" in accordance with Chapter 12 of OPNAVINST 5510.1H. Commands can only distribute technical data according to the distribution statements marked on the documents. Upon receipt of a request for technical data with military or space application, a command must determine if:

A. Requester is a qualified U.S. or Canadian contractor (verified by a DOD approved DD Form 2345).

B. Request is consistent with the business activity as described on the DD Form 2345.

(Refer to OPNAVINST 5510.161)

Freedom of Information Act (FOIA) requests for this type of technical data will be denied citing 5 U.S.C. 552(b)(3). Other requests from non-certified individuals or firms will be denied, offering a fact sheet (provided in OPNAVINST 5510.161) and a DD 2345 to be filled out by the requester and submitted to DLSC if so desired.

Requests from foreign nationals or entities must be referred to the Naval Office of Technology Transfer and Security Assistance (NAVOTTSA-10).

Navy Nuclear Propulsion Information (NNPI) and technical data concerning submarine matters will not be released without the prior approval of OP-OON and OP-02.

To date, approximately 20 denials of controlled technical data have been made to requesters. Problems have arisen due to some confusion on exactly what data falls in the restricted category, and at least one enterprise has taken the Navy to court for denying the information.

Conversely, the president of Newport Aeronautical, a certified contractor, was arrested for attempting to illegally convey controlled technical data to the Government of South Africa without an export license. The Navy temporarily suspended the company's certification but did not submit a recommendation, as required, to the Office of the Under Secretary of Defense, Research and Engineering (OUSDR&E) for final revocation. It was later learned that the information seized belonged primarily to the Air Force, who had never suspended certification and continued to provide Newport Aeronautical with technical data, even after the president's arrest.

There is still confusion about the program, but OUSDR&E is presently drafting a revision to the Department of Defense directive, to identify more clearly what information is protected by this program and emphasizing the legal aspects and reporting requirements.

Specific policy and procedures can be found in OPNAVINST 5510.161, "Withholding Unclassified Technical Data from Public Disclosure" dated 29 July 1985. Questions may be directed to the Chief of Naval Operations (OP 09N2), Washington, D.C. 20350-2000. ★

Handling *'NATO'* documents

by Raymond P. Schmidt, Head, NISCOM Classification Management Branch

"Chief, I just got this message marked 'NATO CONFIDENTIAL.' What's that mean?"

"Show me, Jim. I haven't seen that classification in five years. I don't think we have anyone onboard cleared for NATO."

This scenario, or one like it, takes place several times a month. The Chief of Naval Operations (OP-09N2) wants to make your job easier, and reduce the time needed to brief Navy personnel about NATO classified material. Navy personnel are guided by instructions from the United States Security Authority for NATO Affairs (USSAN) -- the Secretary of Defense.

"NATO material is covered under a special access program, Jim. If we get classified messages marked NATO, we're supposed to brief everybody who needs to see them."

"Where do I find that information, Chief? I never got that training."

"First, check the Navy information and personnel security manual, OPNAVINST 5510.1H. See, it says that we need OPNAVINST C5510.101D to brief our people for access to NATO classified information. But we wouldn't need the briefing if we only got 'NATO RESTRICTED' and nothing higher."

The Secretary of Defense has authorized Navy commands to handle NATO RESTRICTED information in the same manner as we store, transmit, and control U.S. FOR OFFICIAL USE ONLY information.

NATO RESTRICTED information may be stored in filing cabinets, desks, or other containers located in rooms where government or contractor security is provided during non-duty hours. Locked buildings or rooms usually provide equal protection if internal building security is not available.

U.S. unclassified documents that contain NATO RESTRICTED information must identify it by appropriate markings on each page, and on the cover or first page.

Documents that contain NATO RESTRICTED information will be packaged and single-wrapped, and mailed via U.S. First Class Mail.

These and other procedures for safeguarding NATO RESTRICTED information are explained in OPNAV NOTICE 5510 of 17 November 1988. They are also being incorporated into OPNAVINST 5510.1H.

For classified NATO material, OPNAVINST C5510.101D is required. If your command needs this document, a letter request must be sent via your administrative chain of command to the Chief of Naval Operations (OP-09N), Department of the Navy, Washington, DC 20350-2000. (If you need to talk with someone at OP-09N, call the Security Action Line: A/V 288-8856 or commercial (202)433-8856.) The letter must explain why you need the NATO Security Procedures Directive. While awaiting the requested Confidential instruction, classified NATO messages should be seen only by those who need them for action, and should be stored in a proper security container. Most important is to maintain control of the NATO classified material and store it apart from U.S. classified documents, even if locked in the same safe drawer.

"Chief, I see the briefing here in the NATO instruction. Looks easy enough. So now I get everybody to read this briefing, and that's it?"

"Right, Jim. But we need to keep a record of who gets the briefing and debrief them when they don't need it any longer. The OPS Officer is transferring in a few months, so we should be sure to debrief him when that time comes."

Once the basic briefing for handling NATO classified material has been given, no additional action is required for access to other NATO classifications, such as 'NATO SECRET.'

The USSAN is currently preparing a revision to the basic instruction governing NATO security, and the Navy will provide copies to all who need it when the new instruction is approved. Meanwhile, OP-09N2 is providing appropriate *unclassified* portions of NATO guidance to all ships and stations. That guidance should reach users by late 1989.

'But those are just my *personal* notes!'

Oh, really?

by S/A Richard J. Sullivan
NISCOM Damage Assessment Branch

Have you ever...

...attended a Navy school which let you take your classified notes "home" to the ship (or office), provided you marked them, wrapped them and addressed them to yourself at your command?

...prepared a classified document or message and then kept your own "personal" copy "just in case?"

...wondered, a year or two later, just what exactly happened to that copy or those notes you never used?

...looked at your classified notes from a school and wondered just why in the heck you kept them in the first place, or decided that they were never really classified after all?

...held a classified inventory in which you found a packet of "Personal Working Papers" or "Class Notes" for some shipmate you never heard of before?

...heard a shipmate jealously grab a classified correspondence course textbook from someone else, because "that's my personal copy!"?

If you have been in the Navy for more than a week or two and have had anything to do with classified material, chances are you answered "yes" to at least one of these questions. It's common enough: the exercise planner, the author or editor who forgets the simple fact that information, which is properly classified, is never the property of those to whom it is entrusted, and it may not be declassified arbitrarily.

In the past year a number of instances have been discovered in which Navy and Marine Corps personnel have risked the compromise of classified information entrusted to their care. You must wonder if they would deliberately risk their own careers and personal freedom the same way, because that's exactly what they are doing. Time and again, classified correspondence courses are found in vacated apartments, garages, and mini-warehouse storage sites. "Sample messages," tactics notes and study guides, and even sensitive compartmented information have turned up in household goods shipments and packages mailed home. Improperly retained classified material has been discovered by spouses or neighbors in someone's closet, or basement, or even in public dumpsters. Those who have a gripe against the "owners" of the classified material, eventually turn them in.

And these are only the events we hear about. How much more is lost without a trace, and what happens to it? We don't know. So, what is being done to control these unofficial classified documents?

Recently, some training commands have limited the practice of "sending home" classified course notes. OPNAVINST 5510.1H makes it clear that classified information, in whatever form, remains classified and is never anyone's "personal" property. But there are still a lot of "personal working papers" out there for which no genuine need exists and over which we have no real control. And it's not just the recent student or instructor who likes to have a personal copy "just in case." Rare is the security manager who hasn't experienced the mixed emotions of having to remind "the old man" that he can't really take classified material home with him, or keep those old messages for "his book."

And how many of us assume that with the passage of time or public exposure through open press, what was once classified is now "UNCLAS?" Unless information is specifically and officially declassified, even if it has appeared in your favorite newspaper, that information remains classified and must be protected.

If you have such "personal files" of classified material, you must understand that they are not yours to do with as you please. They must be properly protected, and, if necessary, controlled. Finally, ask yourself if you are willing to risk their compromise and your career in return for your

personal convenience. Unless you can properly control and protect that information, the risk outweighs the gain, and your clear responsibility is to properly destroy those "unofficial" and "personal" copies of classified information. Now is the time to seek them out, and destroy them. (Properly recording the destruction, of course.)

DoD and Navy policy are clear on the point that the security of classified information rests with every person to whom access to that information is granted, not just with the "security manager." You are responsible for compliance with policy. Executive Order 12356 requires that classified information will be **"used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons."** It also provides that **"Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions"** for disclosing classified information to unauthorized persons.

What sort of sanctions are applied in the real world? A retired senior chief who removed classified messages, "for his own information" while employed as a GS-05 reproduction machine operator, was recalled from retirement by the Secretary of the Navy, tried at a General Court Martial, and convicted. He lost all retirement benefits, was fined, and imprisoned. Oh, yes, he also lost his job as a repro-clerk. Was this an extreme example? Not really, for such carelessness happens far too often. Just watch the headlines for the next example. Or better yet, do something about it, and destroy those old notes today. ★

Entry and exit inspections...

...many benefits

by M. F. Brown, Head,
NISCOM Information Security Division

All Department of the Navy activities are required to establish an "Entry and Exit Inspection" program. An implementation of a Stilwell Commission recommendation, it is required by DOD Information Security Program Regulation DOD 5200.1R, and OPNAVINST 5510.1H.

A problem, or at least a potential problem, may occur when carrying out this program. What do you do when you discover the unauthorized removal of other-than-classified material when conducting inspections? Can it be confiscated even though the purpose of the inspection is to detect classified material? Yes, you may confiscate any contraband, classified or unclassified, that is discovered during such inspections. The procedures to be followed are the same as those normally used by security officers upon the discovery of a person removing facility property without authority.

Has an entry and exit inspection program been established at your command? Did you know that convicted spy John Walker told federal investigators that he would not have taken the chance of being caught by such a program. That if the Navy had presented him with even a random, remote possibility that he would be searched, he would not have removed classified documents from his workplace. And would have been forced to use other more conspicuous means of obtaining documents...and may have been detected sooner.

Who knows? You may discover that it has beneficial side effects, like reducing pilferage. ★

Security violations..
...who's responsible

by S/A Richard J. Sullivan
NISCOM Damage Assessment Branch

A retired CPO working as a GS-5 "reprographic" clerk at a communications facility had a curious interest in classified messages. Was that an Intelligence Information Report he just put in his wallet?

A sensitive photograph of the latest Soviet aircraft carrier appeared on the front cover of a British Defense Industry magazine. This wasn't a case of "spying for the enemy" but of someone selling classified information to a news magazine. The source of the photograph was identified as a highly trusted employee of the Office of Naval Intelligence (ONI).

Classified information is turning up in trash dumpsters, in private garages, in public archives, in the possession of "friendly" and hostile foreign powers, in the public media, and in case-loads of the Naval Investigative Service (NIS) everywhere. Proper control and handling of classified material has become, in some cases, a nightmare.

Who is responsible for safeguarding this information, who is responsible for losing it and who is supposed to do something about it?

In all cases, the answer is **You !**

OPNAVINST 5510.1H requires all Navy and Marine Corps commands to report all security violations which involve the loss, compromise, or *possible* compromise of classified information to NIS immediately upon initiation of the Preliminary Inquiry. If there is no loss, and a compromise is ruled out, the Preliminary Inquiry may be the only step necessary, but the incident must be reported.

Well, that's what "Navy Policy" says, but is that what really happens? The answer is "Yes, sometimes, but not often enough."

Classified material turns up in the trash, public archives, the media, and in the hands of foreign governments. And <u>You</u> are responsible!

In the case of the retired chief, an enlisted watchstander became suspicious of the repro clerk at an OUTCONUS comm center in WESTPAC. These suspicions were relayed to the Officer-in-Charge who began a Preliminary Inquiry and immediately notified the local NIS Resident Agency. The Inquiry suggested there might be some actual basis for the suspicions, but there was no "solid proof" that the clerk was doing anything wrong. While the chain of command was being notified, NIS requested that all other command investigative steps be held in abeyance so as not to alert the suspect, who had daily access to SECRET traffic. NIS began a long-term undercover investigation which led to the arrest of the retired chief who was caught leaving the base with a classified message in his possession. Searches recovered other classified material from his off-base residence in the host country. He was subsequently convicted by a SECNAV-approved court-martial for passing U.S. Intelligence information to a security service of the *friendly* host government.

Amazingly, while this first investigation was going on, another employee at another comm center at the same command reported similar suspicious activity by yet another GS-5 repro clerk (this time a retired E-8). Another undercover NIS investigation was followed by a SECNAV-approved Court-Martial of a retiree. Another "trusted employee" was convicted of passing classified U.S. information to foreign nationals.

Incidentally, as a result of their General Court Martial convictions, both men lost all their retirement benefits and were sent to prison.

In the case of the ONI employee who "moonlighted" as a photojournalist, the situation was a little different. It seems that he irritated some of his co-workers who either knew or strongly suspected he was violating security regulations. But whose job was it to report his actions? "It's not *my* job" became a common, but sad refrain. One of his co-workers later complained that counterintelligence was too slow. "What took you so long?" we were asked. "Everyone knew that he was a stringer" for the British journal, said the co-worker, who claimed he had been waiting for someone else to do something about it. He himself, of course never told anyone.

Despite the policy, few commanding officers truly relish the prospect of putting themselves on report by notifying the NIS of the loss or possible compromise of classified material, so, some conclude "If we can't *prove* it was lost, then it *wasn't* lost, it's just 'unaccounted for' until we find it." That line of reasoning lead

one ship, which could not account for over 100 classified documents, to conclude that the documents were "probably inadvertently" destroyed. The Type Commander was neither impressed with nor amused by that argument.

At the other end of the spectrum, we do have the folks who leave a safe unlocked for a short time or leave a classified document out on the bridge, when uncleared personnel are present. In those cases, the command must make a judgement call as to whether or not a compromise was possible (assuming nothing was missing or "unaccounted for") given all the circumstances.

So, what kind of violation is serious enough to warrant an investigation? The COMSEC and Sensitive Compartmented Information (SCI) communities use various terms for the distinction they make between "insecurities" or "discrepancies" and "serious" violations.

An **Insecurity** (COMSEC) or a **Discrepancy** (SCI) usually means a breach of the security regulations which govern those communities, but do not necessarily amount to a loss or compromise of classified information. For example, a simple violation of "Two Person Integrity" is a COMSEC insecurity which must, according to CMS 4L, be reported, but may *not* require a Preliminary Inquiry or JAG Manual Investigation unless there is *also* a loss or compromise. An inadvertent disclosure of an SCI procedure may not necessarily also involve a compromise as defined in OPNAVINST 5510.1H. For example, suppose a CONFIDENTIAL document is mailed "registered" mail but is not properly wrapped. It arrives at its destination intact, seals unbroken, but the recipient should report the discrepancy by mailing an OPNAV 5511/51 "Security Discrepancy Notice" to the originator, with a copy to CNO (OP-09N).

You must take notice of and report both major and minor violations, but more serious violations, specifically those which *do* involve the loss or possible compromise of classified information must be investigated. There are three basic types of inquiries or investigations.

A PRELIMINARY INQUIRY is an *administrative* step, intended solely to initiate damage control. It is not a formal fact-finding body, and it is not a criminal investigation. In the Inquiry you must determine whether classified material was lost or possibly compromised. If so, find out exactly what was compromised and how, and immediately tell the "originator" of the classified information. This is akin to a "MAN OVERBOARD" operation, reversing the ship's course and taking muster while the motor-whale boat crew is assembled. Then you notify the ships in company. So too, the originator, CNO (OP-09N) and NIS must be notified as soon as a loss or compromise is suspected. Other details which are "nice-to-have" include identifying the responsible party, getting written statements from witnesses, identifying security weaknesses and recommending corrective steps. But the Preliminary Inquiry Report must never be delayed beyond three days in hopes of answering all of those questions. A supplemental report, if necessary, is perfectly acceptable. If the originator cannot be identified, the message report must be sent directly to CNO (OP-09N).

The **NIS INVESTIGATION** is responsible for resolving questions of criminal culpability or counter-intelligence interest. If there is a loss or possible compromise, NIS must have an unhindered chance to gather and examine evidence. Even if NIS declines investigative jurisdiction, the command is not relieved of the requirement for either a Preliminary Inquiry or JAG Manual Investigation.

A JAG MANUAL INVESTIGATION is an *informal* fact finding body (usually one officer) designed to resolve specific administrative concerns such as what security weaknesses exist, how they can be corrected and whether punitive or non-punitive disciplinary action is warranted. The primary objective is to prevent a recurrence of the same error or violation in the future. The JAG Manual report follows the administrative chain of command but is addressed to the Chief of Naval Operations (OP-09N) and *not* to the Judge Advocate General. The report *may* use information developed by an NIS investigation, including statements (prior coordination with NIS is necessary), but it may not incorporate the complete NIS Report of Investigation. Two important steps most often omitted in the JAG Manual Investigation are the Classification Review and Damage Assessment which are done by the

(Continued on following page)

Violations

(Continued from previous page)

Original Classification Authority or the originator of the lost or compromised material. Requesting these is the responsibility of the investigating officer.

Frequently, when classified material is reported as lost or subjected to compromise, it is later found in the custody of cleared personnel who did not know they had it ("lost in the safe") or who missed it during the "inventory." Recently, a classified item, missing for over a year, was found in the "wrong" vault within a classified space. There was a general sigh of relief, but not much interest shown in finding out how the package came to be misplaced, and most importantly, if it had been there the entire time it was "unaccounted for."

"Okay, so those are nice sea stories, but that stuff doesn't happen every day, and it doesn't happen here in this command."

Well, unfortunately, loss and compromise of classified material happens in the best of families. No community, no ship-type or air-wing, gator or bubblehead, ship driver, plane flyer, seagoing operator or landlocked staffmember is entirely without suspicion.

A classic example of that is the co-worker of our ONI-photographer friend -- the one who complained about how the counterintelligence folks were so slow. Some time later, he found out how the system should work. The co-worker had been assigned to a different work center as an intelligence analyst. He was highly trusted and appropriately cleared with all the "tickets" punched, and he had access to a considerable variety of classified information which he was passing to another "friendly" foreign power. But one of *his* co-workers couldn't understand why the analyst was collecting information which had nothing to do with his duties, for which he didn't really have a "need to know." This co-worker didn't wait for someone else to take action, but reported his concerns to their supervisor. As a result of the subsequent NIS investigation, the curious analyst and his wife were tried in U.S. District Court and convicted of passing that information to another "friendly" foreign nation. Both are in Federal Prison.

It seems to be a problem everywhere, but very much like most other *diseases*, if recognized in time, it can be treated and cured; but if ignored, it festers and grows, becoming more painful and life-threatening. Prevention techniques are important, and in the case of classified information, prevention is education, awareness and individual responsibility. After a loss or compromise, the prescribed treatment is an objective investigation.

Rather than viewing a security violation as a headache and devising excuses or rationales, commanders and commanding officers must examine their own procedures for handling classified material. Then they must convince all hands that responsibility for identifying security violations rests not solely upon the classified custodian, but with everyone.

If you saw a shipmate fall over the side while underway, you wouldn't wait for the fantail watch to report a man-overboard. Similarly, you can't wait for "the other guy" to report a violation or discrepancy either. Not only *can* it happen on your ship, on your watch, but the odds are that it *is* already happening. And on *your* watch, too!

SO, HAVE WE LEARNED ANYTHING YET?

We've learned that the gravest threat to our security comes not from "Boris the Byelorussian Tractor Salesman," but from our own carelessness and complacency. Frequently the weakest link is our unswerving trust in anyone who has not yet been convicted or suspected of espionage.

With the initiation of centralized review of all Navy security clearances at the Central Adjudication Facility, something is being done about standardizing Navy-wide criteria for clearances and access to classified material. We are doing the same thing with security violations and discrepancies.

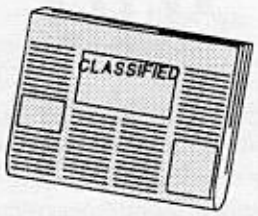
John Walker completed his career without having been subjected to a full-blown security re-investigation. Each of his new commanding officers had no reason to question Walker's conduct, and each new assignment gave him a clean slate. After the arrest, a common observation of his peers was that, in hindsight, *"something"* looked "funny" either in Walker's conduct, his handling of classified material, or in the command's classified holdings; yet no one thought that any single event, taken by itself, was serious. Several people thought it strange that Jerry Whitworth's wife came to pick him up in a Rolls-Royce, but no one asked a few simple questions. As a result, no one was able to put more than one piece of the Walker puzzle down at any one time. Thus, no one even knew there *was* a puzzle to be solved until it was too late, and the ring had moved into its ***second generation*** of espionage within the U. S. Navy.

Another thing we've learned is that it is imperative that every actual or suspected loss or compromise of classified material be properly investigated *and* reported. We must take our personal responsibility to protect classified information, and to recognize insecurities and discrepancies seriously.

A cooperative effort involving both the command and the NIS counterintelligence professionals is the first step. They

EXTRA! EXTRA! Read all about it!

by Suzan A. Cox
NISCOM Security
Review Branch



A compromise in the public media is the disclosure of classified material in newspapers, magazines, books, pamphlets, and radio or television broadcasts. (Refer to OPNAVINST 5510.1H, Sec 4-11)

How do these compromises occur? Most recent disclosures have been through printed media. They can occur when Navy personnel or contractors who have access to classified material, are approached by reporters for comments on various defense-related subjects, and they inadvertently, in the course of the interview, give away classified information.

Compromises also occur when individuals, considered as experts in their various fields, give presentations to open and closed audiences, write opinion papers, articles or studies on topics within their areas of expertise, and include sensitive or controversial facts and figures. The Navy has a multitude of these "experts," ranging from technical subjects such as electrostatic ion instabilities in various conditions, to broader subjects such as the role of the fleet in the 1990s. These 'experts' are scattered throughout the Navy and its contractors.

Often such people are under the impression that if they cite unclassified sources, it is alright to publish what they wish. Wrong! Just because, for example, the range of a new missile appears in *Jane's Weapons Systems*, does not mean that the information has been officially released.

The situation becomes dangerous when a well-known "expert" in a particular field, whether consciously or unconsciously, selects sources which come closest in accuracy to classified sources, and inadvertently lends credence, by virtue of his position, to information in the public domain that the Navy considers classified.

Anyone having access to classified information should be aware of the risk in dealing with the media. The smallest, most seemingly inconsequential piece of information may enable an adversary, who is following the program closely and can view that information in a larger context, to thoroughly understand a concept, developing an unfair advantage over the U.S. and an ability to develop countermeasures.

It is essential to the effectiveness of our Information Security Program that when preparing for an interview or gathering material for inclusion in an article or other product for the public domain, that only officially released facts and figures be used.

Once a compromise has occurred, the Chief of Naval Operations (OP-09N2) must review the material for a damage assessment and recoverability estimate. Depending on the amount of the material and level of classification, it may be necessary to completely reevaluate an entire program to determine if the disclosed information can be officially released. This takes many man-hours away from more productive and positive efforts.

Observe proper prepublication security review procedures. It's one way each of us can do our part to enhance the Navy's Information Security Program. ★

can provide a plethora of advice and support from security briefings, to the Pro-Active Counterespionage (PACE) program, to full scale investigations.

When there *is* a loss or suspected compromise, OPNAVINST 5510.1H requires that a Preliminary Inquiry be initiated and that NIS be notified, and that the report be forwarded to CNO (OP-09N) whether or not NIS investigates. At OP-09N all the reports are reviewed, analyzed, and contrasted with the JAG Manual Investigation, NIS investigations and other available data to determine what has been compromised. The compilations of losses, compromises and known or suspected hostile intelligence service Essential Elements of Information can identify areas which require greater protection and may well identify heretofore unknown vulnerabilities to espionage. From this data, we expect to learn what our vulnerabilities are and how we can protect ourselves, not just from "them" but from ourselves, too. Once identified, weaknesses *must* be corrected, for if ignored, they can devastate us.

To make this system work, we need a realistic understanding of the policy, and Navy-wide compliance with that policy. And "Navy-wide" starts with you and me. ★

Why a security review?

by Janet Vaccaro
NISCOM Security Review Branch

"Why is security review so cumbersome and complex? I'm just trying to have my article published in next month's journal. Is it really necessary that my draft go through the scrutiny of a security review? I don't think there's anything in it that would pose a threat to national security if it's printed. Besides, it always takes so long to get an article cleared for public release."

These are the words of a frustrated Navy Commander, anxious to have his written work published. His area of expertise is mine warfare, and even though his article only speaks in general terms about his work, it must be submitted through the chain of command before it can be approved for public release. Much of his frustration about the security review process stems from a lack of understanding of it.

The origin of security review is Executive Order 12356, which gives the Department of the Navy (DON) the authority to protect from unauthorized disclosure any classified information. Anything submitted through the proper channels for a security review will be approved for public release only if it is consistent with the interests of national security.

Technical papers, speeches, manuscripts, articles, films, and videotapes are among the materials the DON is responsible for reviewing prior to public release. Active duty and reserve components, DON civilian personnel, and DOD contractors must submit proposed works for a prepublication review. Retired persons are not subject to this requirement, but are encouraged to utilize the security review process.

The first step in this process is an internal command security review. Many documents can be examined at the command level and found suitable for public release without any higher level consideration. Each command has an official who is responsible for making certain a proper review of this material is completed. In most activities, it is the duty of a public affairs officer (PAO) or a security manager. If clearance cannot be granted at the command level, the PAO or security manager will submit the material to the Chief of Naval Operations, OP-09N2, or the Commandant of the Marine Corps (Code INTC) for Marine Corps matters, for further review.

OP-09N2 coordinates the review of the information with cognizant authorities. Cognizant authorities are officials who have program or technical knowledge of the material proposed for release. OP-09N2 tasks such officials to examine the material and identify any classified information. Reviewers are instructed to use classification guides provided by the OPNAVINST 5513 Series and any other relevant source material when deciding if security amendments are required. OP-09N2 also provides an analysis of the information in light of the reviewers comments to assure consistency with the classification guides, to prevent arbitrary decision making, and make the fewest alterations necessary to ensure protection of national security.

In most instances, the information will require a review by the Office of the Assistant Secretary of Defense Public Affairs (OASD/PA). OPNAVINST 5510.1H lists the categories of information which require review and clearance by OASD(PA) prior to public release. OASD(PA) works closely with OP-09N2 and functions in a similar manner. OASD(PA) provides the final determination as to whether material will be released to the public.

Any individual has a right to appeal decisions made by OASD(PA), or a lower authority. The appeal should include a justification of why the material is suitable for public release as well as official unclassified sources of the information.

The DON encourages its personnel to generate articles, manuscripts, etc., and no author should feel this process will infringe upon his creativity. The following suggestions will facilitate the security review process.

Familiarize yourself with the directives. Applicable guidance is found in OPNAVINST 5510.1H, SECNAVINST 5720.44A, and MCO 5510.9A.

Don't assume that because something is in print, it's unclassified. There are many published works which never received a security review and were never officially approved for public release. Such documents are not valid unclassified sources.

Submit all work proposed for public release. Remember, even if it remotely deals with a Navy topic, it could have security implications if released to the public.

Conform to submission requirements. Submit six copies of the work for review.

Allow enough time for an adequate review. Allow at least four weeks (not including mailing time) for a security review to be completed. Length of material, complexity of content and other mitigating factors impact review time.

New security specialists in place

Information and Personnel Security personnel have been assigned to the Naval Investigative Service Regional Offices (NISRO) in Pearl Harbor, Mid-Atlantic (Norfolk), and London. Their duties include organizing security training seminars, conducting briefings, supporting IG inspections, interpreting security directives, visiting activities in assistance roles, and developing security plans. These Information and Personnel Security Specialists complement the Law Enforcement and Physical Security (LEPS) Assistance Teams in their respective regions.

George L. Jackson
NISRO Pearl Harbor, Hawaii
Box 76, Pearl Harbor, HI, 96860-7200
AV: 431-0111 (ask for 471-8473)
Comm: (808) 471-8473

Robert C. Allen
NISRO Mid-Atlantic Region
Norfolk, VA, 23451-6498
AV: 565-2247
Comm: (804) 444-2247

Ronald Bell
NISRO Europe
Box 11, FPO New York, NY 09510-3000
AV: 01-868-2457

RANKIN update

New and revised directives

by Ronald Marshall
RANKIN Program Manager

So far this year, the following classification guide series have either been created or revised:

OPNAVINST 5513.14, Department of the Navy Security Classification Guidance for Space Programs, dated 10 March 1988.

OPNAVINST S5513.4C, Department of the Navy Security Classification Guidance for General Intelligence, Cover and Deception, Security and Investigative Programs, dated 13 July 1988.

OPNAVINST S5513.13A, Department of the Navy Security Classification Guidance for Non-Acoustic Anti-Submarine Warfare Programs, dated 19 September 1988.

The next series to be promulgated will be **OPNAVINST S5513.8B**, Department of the Navy Security Classification Guidance for Electronic Warfare Programs. That series is nearing completion and should be distributed about March 1989. The revision will include new guidance on the AN/WLQ-4(V)1, an advanced signal exploitation system, and the AN/WSQ-5(V), a countermeasures receiving set. Two additional guides implement new JCS guidance on Wartime Reserve Modes and new DOD guidance on High Power Microwave Technology.

Following the revised OPNAVINST S5513.8, guide users can expect a revised **OPNAVINST S5513.6C**, Security Classification Guidance for Communication and Satellite Programs around May.

Copies still remain of **DOD 5200.1-I**, the DOD Index of Security Classification Guides. This index is useful to program managers to determine whether there exists classification guidance that may be relevant and adaptable to their systems, programs, plans, and projects and, if such guidance exists, where to find it. Use of the Index is necessary to avoid divergent security classification determinations between the components over like information.

If you need assistance regarding DON classification guidance, or would like a copy of the DOD Index, the RANKIN Program Manager, Mr. Ronald W. Marshall, may be reached at Commercial (202) 433-8861, or Autovon 288-8861. ★

No clearances for non-citizens

by Mary Ming, Head
NISCOM Personnel Security Division

Only U. S. citizens are eligible for a security clearance. Immigrant aliens and non-U. S. citizen (foreign national) personnel may not be granted clearances and should not be employed in duties that may require access to classified information.

Enlisted foreign nationals may not enter ratings or Military Occupational Specialities which generally require security clearances. In the past, Philippine nonimmigrant aliens on active duty were authorized, by exception, to be considered for Confidential security clearances. Under the new personnel security policy, they are no longer eligible for such consideration -- however, they may be considered for a Limited Access Authorization (LAA).

Each security clearance that was granted to a Philippine nonimmigrant alien or other foreign national under previous policy must be reviewed to determine whether the conditions for LAA apply. If an LAA appears to be justified, a request may be submitted in accordance with paragraph 24-6 of OPNAVINST 5510.1H as soon as possible. The clearance entry on OPNAV Form 5520/20 must be annotated with the date the LAA request was submitted and clearance may be retained until response to the LAA request is received. If the command cannot justify an LAA, the security clearance must be administratively withdrawn immediately and the OPNAV Form 5520/20 annotated accordingly.

When there are compelling reasons to grant access to classified information to non-U.S. citizens in furtherance of the Department of the Navy mission, including special expertise, foreign nationals may be considered for an LAA under the following conditions:

1. LAAs must be limited to the Secret and Confidential levels only; LAAs for Top Secret are prohibited.

2. Access is limited to classified information relating to a specific program or project.

3. Disclosure authority determines that access to classified information is consistent with releasability to the individual's country of origin.

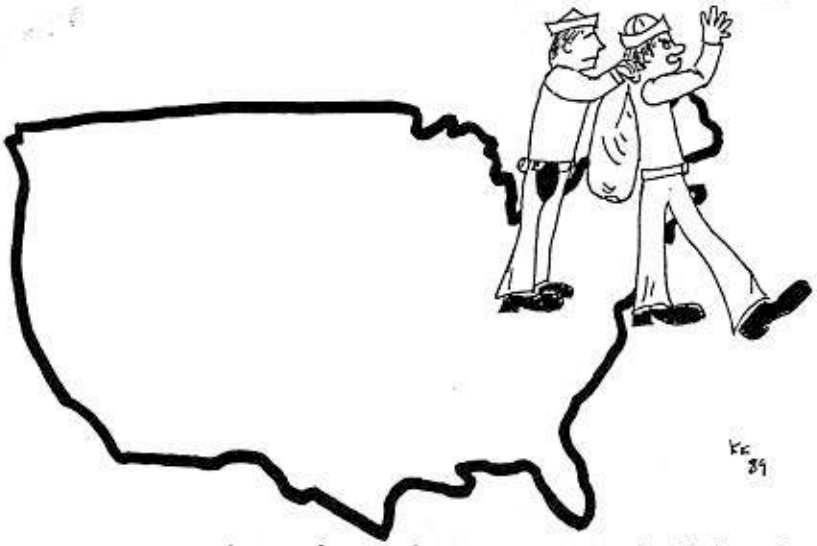
4. Access is based on favorable completion of a Background Investigation (BI) scoped for 10 years; where full investigative coverage cannot be completed, a counterintelligence-scope polygraph examination will be required.

5. A foreign national employee must agree to a counterintelligence-scope polygraph examination before being granted access.

Requests for LAA must contain the identity of the individual for whom LAA is requested, including name, date and place of birth, current citizenship, social security number (if held), status (immigrant alien or foreign national); date and type of most recent personnel security investigation (If a BI has not been completed within the past five years, the forms required for BI must be enclosed); level of any security clearance granted under previous policy; the position requiring access and the nature of the specific program material (delinated as precisely as possible) for which access is requested; the compelling reasons for the request; the expected termination of the LAA; and a statement that the candidate has agreed to undergo a counterintelligence-scope polygraph examination when needed.

These requests must be submitted to CNO (OP-09N2). ★

Catch 'em in CONUS



by Mary Ming, Head
NISCOM Personnel Security Division

Personnel security investigations overseas are difficult to complete in a timely manner. To expedite these investigations prior to deployment or transfer overseas, the Defense Investigative Service (DIS) has developed the "Catch 'Em In CONUS" (CEIC) program to reduce completion time and number of overseas lead requirements on Special Background Investigations (SBIs), Background Investigations (BIs), and Periodic Reinvestigations (PRs).

This program facilitates direct communication between the command security manager and the servicing DIS office. It enables DIS agents to conduct military reference interviews and command related inquiries on ships/squadrons preparing to deploy and aimed at accomplishment prior to the individual's departure for an overseas permanent change of station (PCS) or long term deployment.

Security clearance request packets should be submitted at least 90 days prior to any scheduled long-term deployment or overseas PCS. However, those requests that become known to the command with less than 90 days remaining may be submitted by utilizing CEIC procedures. DIS advises that the "Catch 'Em In CONUS" program can and should be employed even when almost no advance notice of a movement is provided. In many instances, DIS may be able to have an investigator on the scene immediately.

To assure consistent and orderly case processing for any personnel making a long-term deployment or overseas PCS move requiring a Top Secret clearance, the following procedure should be followed:

The personnel officers, commanders or security managers must identify personnel eligible for "Catch 'Em In CONUS" SBI, BI or PR as soon as possible.

The individual scheduled for PCS overseas or long-term deployment should complete Personnel Security Questionnaire (DD Form 398), Applicant Fingerprint Card (DD-258), and Authorization for Release of Information and Records (DD Form 2221) and submit them to the requester of the investigation.

The base-authorized requester should initiate a security clearance request packet 90 days prior to departure.

The request packet consists of the following forms:

a. Original and two copies of Request for Personnel Security Investigation (DD Form 1879);

b. Original and four copies of DD Form 398;

c. Original and two copies of National Agency Check (NAC) Request (DD Form 398-2) *for spouse if request is for SBI and a prior NAC had not been conducted previously.* (No spouse NAC is required for BI or BI-PR);

d. Two copies of DD-258;

e. One copy of DD Form 2221.

The requester initiates a CEIC request for investigation by notifying the local DIS agent by telephone. A suspense copy of all request forms should be retained for forwarding to the gaining command in the event the SBI, BI or PR is not completed before the subject's PCS move.

The DIS agent will pick-up packets and review them for accuracy and completeness, conduct the subject interview and follow-up local leads. The agent then forwards the request to DIS headquarters for processing and completion of other necessary leads. ★

STOP!

Don't use SF-86...yet!

The Office of the Under Secretary of Defense for Policy has advised that Navy activities should not use the new Questionnaire for Sensitive Positions (SF-86 (Rev. Oct 87)) pending a final decision by the Office of Personnel Management (OPM) concerning the listing of **five** vs **15** years for the background investigation. SF-85 (Rev. Feb 66) Questionnaire for Non-Sensitive and Non-critical-Sensitive National Agency Check Investigations (NACIs) should be used until guidance is provided on the new forms.

The Office of Personnel Management (OPM) issued Federal Investigation Notice 88-6, which extends the date for required use of the SF-86 from 16 Sep 88 to 1 Apr 89. Beginning 1 Apr 89, all SF-86s completed in conjunction with a NACI for a noncritical-sensitive position will be submitted to OPM-FIPC, Boyers, PA 16018.

SF-85 (Rev. Dec 87) was recently approved by the Office of Management and Budget (OMB). The new SF-85 is expected to be available for use by 1 Apr 89 with a revised required use date of 1 Oct 89. In accordance with the Federal Investigation Notice 88-6, all NACI requests for nonsensitive positions submitted via SF-85 must also be accompanied by a copy of the Application for Federal Employment (SF-171 (Rev. 2/84)).

Commands should order these forms through their FEDSTRIP/ MILSTRIP ordering system per NAVSUP-PUBs 437 and 485, and DODINST 4140.17M. Also see NAVSUPPUB 2002 (available on microfiche only).

SF-86 (Oct 87) should be used after resolution of the 5 vs 15 years question or by 1 Apr 89. The stock number is 7540-00-634-4036. The stock number for the Continuation Sheet for Questionnaire for Sensitive Positions (SF-86A) is 7540-01-268-4828.

"***Requesting OPM Investigations***" (Oct 87) (Pamphlet OFI-15) has been designed to answer questions on the automated system and contains instructions on how to fill out the "Agency Use Only" block on SF-85 and SF-86. If you have not received this pamphlet, contact OPM-FIPC, Attn: Supply Clerk, Boyers, PA 16018 or call (412) 794-5228.

The importance of DD-398

Defense Investigative Service (DIS) is the single personnel security investigative agency for the Department of the Defense (DoD) including the military departments, defense agencies and DoD contractors.

The term Personnel Security Investigation (PSI) describes an inquiry by an investigative agency into an individual's activities for the specific purpose of making a personnel security determination.

To conduct the required investigation, it is necessary that the investigative agency be provided certain relevant data concerning the subject of the investigation. It is incumbent upon the subject of each personnel security investigation to provide, to the greatest extent possible, required personal information.

At a minimum, the individual must complete the appropriate investigative forms (DD 398 for conduct of a Background Investigation (BI), Special Background Investigation (SBI) or Periodic Reinvestigation (PR) and DD 398-2 for conduct of a National Agency Check (NAC) or Entrance National Agency Check (ENTNAC) for first term enlistee), provide fingerprints of a quality acceptable to the Federal Bureau of Investigation (FBI), and sign DoD Authority for Release of Information and Record (DD Form 2221).

DIS claims that they have encountered a problem in completing questionnaires by members of the Reserve. Frequently, no information is included on the forms concerning unit of assignment, duties or locations, in conjunction with the conduct of a NAC, BI, SBI or PR.

Item 12 of DD Forms 398 and 398-2 must reflect each current or former military assignment of all Reserve members. The directions for this item stipulate that full or part-time employment be listed. The inclusion of this information on the security questionnaire is essential in assisting DIS in conducting a comprehensive and timely investigation. Otherwise, investigation requests may be rejected or an incomplete investigation will be conducted, which may result in inaccurate findings. In both instances, it could cause delay in the investigation processing. ★

Navy dogs invade Panamanian jungle

MWD teams aid Marine patrols defending Arraijan Fuel Farm, in skirmishes with intruders

by JO1 John S. Verrico
NISCOM Public Affairs Assistant

In April 1988, armed intruders were discovered on the Arraijan Fuel Farm, four miles from Naval Station Panama Canal, Rodman, Panama. Members of the Marines' 3rd Battalion, 4th Regiment, "I" Company engaged the intruders in an exchange of fire. One Marine was killed. This was the second incident of hostile fire in 1988.

Naval Station Panama Canal, located in the center of political unrest, had been experiencing frequent incidents of unauthorized entry. In some instances intruders were 'jumping the fence' in the surrounding jungle in what is believed to be attempts to burglarize the Marine Corps Exchange and other facilities. But other intruders, some of them armed, were sighted near the fuel depot. None of the intruders had been captured and their identities were unknown, as were the motives behind the intrusions near the fuel depot.

Marines from the Atlantic Fleet Antiterrorism Security Team (FAST) were deployed to Panama to beef up security and began making regular patrols of the jungle area surrounding Arraijan.

On 15 May 1988, four Navy patrol dog teams were sent to assist with security throughout the Naval Station.

First Class Master-at-Arms Joseph D. Whipple and his Belgian Malinois, Rex, from Naval Air Station Fallon, Nevada; First Class Boatswain's Mate Frank W. Downs and Dejone, a Belgian Malinois, from Naval Air Station Miramar, California; and First Class Master-at-Arms Linda R. P. Cornett and Robby, a Belgian Shepherd, from Naval Weapons Station Yorktown, Virginia, were among the first to arrive. First Class Master-at-Arms Edward T. Croissant, between duty stations at U.S. Naval Air Station Bermuda and Naval Air Station Oceana, joined the group later with J.J., a German Shepherd. The teams would remain in Panama until the facility received it's own MWD teams in late August.

The dogs' superior sense of smell and hearing enabled security patrols to find things and detect intruders where they could not do so before and the advantage of having patrol dogs was soon realized. Whipple, Downs and Croissant, with their dogs, joined the Marines during day and night patrols at Arraijan. Cornett, the only female in the group, was not initially allowed to participate in the Arraijan patrols because it was a potential hostile-fire area. She and Robby at first performed perimeter patrols and other security functions at the naval station, and later was given opportunity to participate in jungle patrols.

The jungle was a completely new experience for these sailors and their dogs -- it was hot, humid, thick with undergrowth and slick with mud from frequent heavy rains.

"The Marines don't believe in following trails," Downs commented, on the Marine Corps habitual avoidance of established

A Navy dog alerts toward an area of thick brush during a jungle patrol in Panama. BM2 Harold W. Garms and his Rottweiler are one of the permanent MWD teams now assigned to Naval Station Panama Canal. (Photo by BM1 Frank W. Downs)

trails and preference for moving through the roughest terrain. "They make their own to avoid ambush and booby traps...The mud was bad. You would climb half way up a hill, then slide all the way back down again.

"I learned a lot down there," he said. "It was a whole new environment for us. When I first saw the jungle, I swore my dog wouldn't do it...but it wasn't the dogs who needed to adjust -- it was us!"

"Robby made a believer out of me!" Cornett said of her dog's performance in the jungle. "He even climbed a tree...A dog will do anything!"

Rex earned the title "Wonder Dog" in Panama. Whipple and Rex performed many night patrols, and in the jungle, night is synonymous with black, as the canopy keeps out any traces of moonlight. Whipple related his first night patrol where he had actually bumped into the man walking in front of him in the darkness. "I stopped and apologized and he had said 'No problem,'" Whipple said. "I only had turned away for a moment, then looked back at where I knew he was standing and waited for him to move again. But he didn't. After several minutes I finally asked him what the hold up was and why we weren't moving on. I got no answer. That's when I realized I was looking at a tree."

In the jungle at night sound is distorted and Whipple had not heard the patrol move on. "I was scared...the first thing they had told me was not to get separated and here I was far behind them. I turned to Rex and said, 'Find them.' Rex put his nose to the ground and we were soon back with the rest of the group."

On several occasions, Rex was used to find people that had become separated from the rest of the patrol, a common occurrence in the blackness of the jungle. "Rex just put his nose to the ground again, backtracked and found them, then brought us all back to the group again...everyone just started calling him 'Wonder Dog,'" Whipple said.

The 'excitement' didn't stop with being in the jungle. During a routine night patrol on 19 July an accidental discharge spooked a group of intruders who, in their attempt to run away, ran into another platoon of Marines. Shots were exchanged between the groups until a grenade ended the skirmish. When the smoke cleared, Downs' dog, Dejone alerted again in another direction and another intruder was found. When he realized he had been seen, he ran. Shots were fired, but the intruder escaped. Downs was present during a similar skirmish on 22 July. Both Downs and Croissant were involved in another fire-fight on 2 August when a 12-man patrol fired at another group of intruders. Croissant himself fired 20 rounds in that incident.

Although Whipple and Rex did not get directly involved on the front line during these situations, they did help by playing an important role. Whenever a hostile force was engaged in fire, Whipple and Rex would go with a another group of Marines into the jungle in an attempt to locate possible points of retreat.

MA1 Edward T. Croissant and J.J. stake out an area in the dense jungle area surrounding the Arraijan Fuel Farm at Naval Station Panama Canal. (Photo by BM1 Frank W. Downs)

It was very exciting, all the handlers agreed.

A temporary kennel had been set up at the naval station for the visiting dogs and plans were in the works for a permanent facility to be built for future MWD teams.

"The can-do attitude and professionalism of the men and women of the Navy's Military Working Dog program were exemplified in the performance of this mission," a CINCLANTFLT representative stated. "We can all be justly proud of the work and efforts of these individuals who with almost no notice were placed in combat vs law enforcement positions."

By mid-August the naval station's permanent MWD teams started to arrive and after turn-over and training, the temporary teams began cycling back to their regular duty stations. ★

by JO1 John S. Verrico, NISCOM,
as told to by MA1 Linda R. P. Cornett,
NWS Yorktown

When I arrived at 3rd Battalion's main camp for the morning's briefing, I felt a little ridiculous -- covered with body armor and web gear, a .45 caliber pistol on one side and a MK-3 knife on the other, a camouflaged steel helmet balancing on my head -- sort of like a child playing 'soldier.'

But as I sensed the weight of all the gear loading me down, I realized this was not a game. It was a time to pull together all of the training I have received and put it to work.

The briefing covered the route we would be taking and our mission for the day. Departure time was set for 1200. After the briefing I practiced all the appropriate hand signals with my Belgian Shepherd partner, Robby, and the rest of the group. By 1145, I was gobbling down my MREs and starting to apply masses of green and brown paste all over my face.

At noon, camouflaged and ready, I got in line with the patrol and began

Jungle Patrol!

One dog handler's rewarding experience

our journey along the east side of the fuel depot. There were eight of us, each with their own special job to perform.

When we reached our first check point and radioed that we were entering the jungle, the tension and excitement mounted. "I was really going in there," I thought as the significance of the mission struck home. Naval Station Panama Canal was in an area plagued with political unrest and armed intruders had been seen on several occasions. No one was sure who the intruders were, nor the ultimate purpose of the infiltration. The Marines who were stationed here to protect the Arraijan Fuel Farm were making regular patrols of the jungle surrounding the base. Now I was joining them.

The jungle was a hot, humid and dreadful place. Little light penetrated the tangle of vines and branches in the jungle's canopy. At night it was an inky void -- the trails couldn't be seen at all in the endless blackness. And it was quiet. You could hear a monkey rustling through the thick branches or a snake slither along its belly in the heavy undergrowth. A myriad of insects provided a continuous buzzing in our ears.

"Watch out for that snake," someone whispered almost too late. One of the many local varieties of poisonous snakes was only inches from my foot. Almost instinctively I reached down and decapitated the reptile with my knife before he could do any damage.

When we reached the next check point, the group halted. Several of the others had encountered a nest of fire ants and had to cast off some of their gear to shed the insects.

I positioned Robby upwind of the rest of the patrol and watched for any changes in his behavior signalling the approach of intruders. You couldn't see far into the jungle around us and you never knew when or if anyone else was nearby. The presence of patrol dogs, like Robby, gave us more of an edge.

The humidity was trapped under the jungle foliage and we all needed to cool down and drink some water before we moved on.

We hadn't gone far before Robby gave an alert down a trail off to our right. I signalled for a halt and informed the patrol leader of Robby's reaction. I took one of the Marines with me and we started down the trail with Robby as point.

He led us to an area which appeared to be a central campsite used by intruders. As Robby took us around the site we found a palm tree that had been cut about twelve feet from the base. The leaves had been used to make a shelter for protection from the rain. Robby led us further where we noticed a spot on the ground where fires had once been built. Several trails led away from the spot in different directions.

By now I had lost my sense of direction and had to rely on Robby's ability to take us back to the patrol.

"Okay, boy. Take us back." He looked around and darted up one of the trails. A few minutes later we were back with the rest of the group, our findings plotted on the platoon leader's map.

The humidity was taking its toll on all of us as evidenced by the sweat dripping from every brow. My camouflage blouse was soaked and the body armor was getting rather uncomfortable. Each step we took was more tiring than the one before, but our mission wasn't over. As we continued to follow the main trail, up and down hills and through the thick jungle brush, my legs began aching. Robby also appeared to show signs of wear, as did the Marines. When we finally reached our last check point the camouflage paint had been practically washed from our faces by sweat.

As we came out of the jungle I felt a great sense of accomplishment. Robby and I had really seemed to make a difference -- to add to the outcome of the mission -- and I was proud.

As Neal Armstrong once said, "One small step for man, one giant step for mankind." Or should I say '*woman*kind.' ★

Because she is female, MA1 Cornett was faced with many concerns about her participation in patrols of the jungle around Arraijan Fuel Farm, which was considered a potential hostile-fire zone. During the first month of their assignment to Panama, Cornett and Robby mostly spent their time performing perimeter patrols. But the success of the other teams proved the benefits of having dogs assist in the patrols, and the insistence by the other dog handlers that Cornett's abilities were equal to theirs helped convince the officer in charge that she could handle the situation. Eventually, she was allowed to join the Marines in the jungle at Arraijan. She proved their faith in her, completing four successful jungle patrols, and became the first known Navy female dog handler to go into a potential hostile-fire area. She thanks her fellow dog handlers for their support in giving her the "opportunity of a lifetime."

Rex covers one suspect while MA1 Joseph D. Whipple searches another in this dramatization of a recent incident where the patrol dog may have saved his handler's life by locating and covering a second man hiding in the sagebrush at night -- only eight feet away from the unwary sailor searching a prisoner in the Nevada desert. (Photo by Jim Ricks, NAS Fallon)

Dogs in the desert -- training's the key

by CDR Olin D. Briggs
Public Affairs Officer, NAS Fallon

Everybody knows the old saw about a man's dog being his best friend, but if you're a Navy dog handler that adage is engraved in steel.

Take the recent case of First Class Master-at-Arms Joseph D. Whipple who took his patrol dog into the sagebrush desert aboard Naval Air Station Fallon to find a suspected felon who was hiding in the sand. He found his man in the dark, but it was his partner who found the second suspect that no one knew was there.

"Standing out there in the field covering my man, I had probably the most scared moment of my life when I finally realized that Rex was covering a second suspect no more than eight feet away," Whipple said.

By doing all that a good Military Working Dog (MWD) is supposed to do, and finding the other man, there's a good possibility that Whipple owes his life to his Belgian Malinois partner.

When Whipple works with Rex it's hard to tell who's in charge.

"We don't work that way, we're a team," Whipple said. "Each of us takes turns leading. We play off against each other to accomplish our mission."

After a six-year stint in the Army, Whipple came to the Navy specifically to work with the Military Working Dog Program.

From the moment he reported to the MWD training school at Lackland AFB in San Antonio, Texas, the six-foot, 215-pound Whipple knew he had found his milieu.

"We learned the psychology of the dog first -- what he needs, when he should eat, sleep and become a kind of mini-veterinarian so that we could take care of our partner the right way," he said.

"Most is plain common sense. The bottom line is simply that the better the handler responds to the dog, the more valuable the team is to the command."

The Fallon assignment was a tough start. The station is geographically isolated and Whipple was originally the

only person working in the MWD program.

His first dog, Flash, a straight drug detector dog who now works with Second Class Aviation Structural Mechanic (Equipment) Kerry D. Weeks, the other MWD handler at Fallon. Weeks was selected for conversion to the Master-at-Arms rating by the October 1988 selection board.

Even though there have been few actual arrests on drug offenses, Capt. Ray Alcorn, Fallon's Commanding Officer, is convinced that the MWD drug prevention program is a success.

"The presence of the MWD team is an active deterrent," Alcorn said. "In law enforcement terms, it's comparable to the patrol officer parking his police cruiser in his driveway at his home -- just knowing the law enforcement presence is there discourages wrong doing."

Continual training is the key. The prerequisites for this training: (1) patience; (2) knowledge; and (3) practice.

Under an arrangement with the Nevada Drug Enforcement Agency, weekly proficiency sessions are held in a cooperative training program.

The dog handler for the El Dorado (California) Sheriff's Department, Terry Fleck, also jumps into this training evolution with his dog, Dirk, whenever he's not busy with Search-and-Rescue (SAR) missions in the Sierra Nevadas.

Rex also gets occasional SAR training, but is not provided any training on sniffing out explosives.

"You could teach a dog to find explosives as well as drugs, but you would not know which one he has found. You don't cross the boundaries here!" Whipple commented.

Rex and Whipple concentrate on crowd control, crime suppression (patrol), building searches, riot control, and similar functions.

"When patrols find an open door in a building, they send for us," Whipple said. "That's the scariest moment for a patrolman, having to go through an open door into a darkened room.

"We announce that anyone in the building should come out immediately or we will release the dog," Whipple said. The spiel goes like this: "The dog will find you and he will bite you. There's no use in hiding."

Whipple said he would much rather conduct a building search with Rex off a leash than with a fellow patrolman.

"If I had to go through an open door I would present a target 6-feet tall and 215 pounds wide," he said. "Rex is one-third my height and body mass -- he's a smaller target. In addition, the dog strikes a spasm of fear in a felon's heart that a patrolman doesn't...it's the morbidity factor, the gruesome consequences of being attacked by the dog."

If the incident in the sagebrush was the scariest one for Whipple, an incident in Hanger 300 made him the angriest.

"We were searching a locker with Flash when the suspect, who had been very nice up to that moment, came unglued and kicked my dog and assaulted me," Whipple said. "It didn't bother me that he shoved me, but it did tighten my jaws that he lashed out at Flash...He was lucky that it was the drug dog that he attacked and not Rex. Rex would have amputated his foot."

Among the many experiences with the dogs, there are incidents that MWD handlers would just as soon forget -- such as the time that Flash answered the call of nature on a sailor's sea bag while a drug check was being held at the transient hanger. The sailor turned out to be a dog lover and was tolerant and understanding.

During another incident, while on a joint training venture with California and Nevada law enforcement officials, the group was having lunch in a fast-food restaurant.

"One of our group always takes care of the drug training aids that we use with the dogs," Whipple recalled. "The place was packed and while we were at the counter ordering, one of the civilians came in and asked: 'Who has the aids'?"

"'I've got the aids,' one of our guys said, (and) boy, did that place empty out in a hurry. By the time that we understood what was happening, we tried to explain, but nobody was listening," he said.

But the seriousness of the mission overrides the moments of levity.

"Fallon's tough on us and the dogs," Whipple summed it up. "The extreme heat of the summers and the extreme cold of the winters are challenges, but the toughest factor to deal with at Fallon is the altitude. At 4,000 feet neither the human body nor the canine body works as well as they do at sea level. It's obvious in just routine patrol work, but it's amazingly obvious when Rex and I go out and run around the 9.6 miles of perimeter fence at the air station four times a week." ★

Flash, NAS Fallon's drug detector dog, locates drugs hidden under the bumper of a car. (Photo by Jim Ricks, NAS Fallon)

Privacy

A relative term

by Lt. Robert C. Wyda, NISCOM Asst. Staff Judge Advocate & MA1 Thil D. Hurley, Former NISCOM Asst. for MA Programs

Search and seizure is an important tactic in investigating and prosecuting crime. While this all-important investigative tool may seem like an invasion of privacy, privacy is a subjective term. What one person may feel is a violation of their rights is not necessarily what the general public would feel in the same situation.

The key to conducting lawful search and seizure operations rests in the ability to identify what a legitimate expectation of privacy is, and what the general public will feel is objectionably reasonable.

In two recent cases, the Supreme Court said no search warrant was required because the "expectation of privacy" was **not** reasonable and there was no violation of rights.

In California v. Greenwood, 486 U.S. __, 108 S. Ct. 1625 (1988), the police, acting on information that Greenwood might be involved in narcotics trafficking but lacking probable cause to obtain a search warrant for his residence, arranged for the retrieval of Greenwood's garbage. Police found that the garbage bags, which had been left on the curb in front of Greenwood's house for regular trash collection, contained evidence of drug use and on this basis were able to obtain a warrant to search his house where quantities of cocaine and hashish were subsequently seized.

At trial, Greenwood contended that the search of his trash bags was unreasonable and therefore illegal.

A two-step analysis is now being used by the Supreme Court to determine if an unconstitutional search and seizure has taken place. The first step asks whether the defendant has a subjective expectation of privacy in the area being searched. If the answer is "yes," then the next step asks if that expectation is acceptable to society as objectively reasonable. A "yes" to both questions indicates that an unreasonable search has occurred, unless a valid search warrant had been issued.

In Greenwood, the Court conceded that the defendant may have had a subjective expectation of privacy in the contents of his garbage bags. But, since the defendant voluntarily left the trash for collection in an area particularly suited for public inspection, his claimed expectation of privacy was not objectively reasonable. The Court noted that it was common knowledge that plastic garbage bags left on the street are readily accessible to "animals, children, scavengers, snoops, (or) other members of the general public." In addition, the reason the refuse is placed on the curb is for conveyance to a third party -- the trash collector -- who may sort through the garbage himself, or permit others, such as the police, to do so.

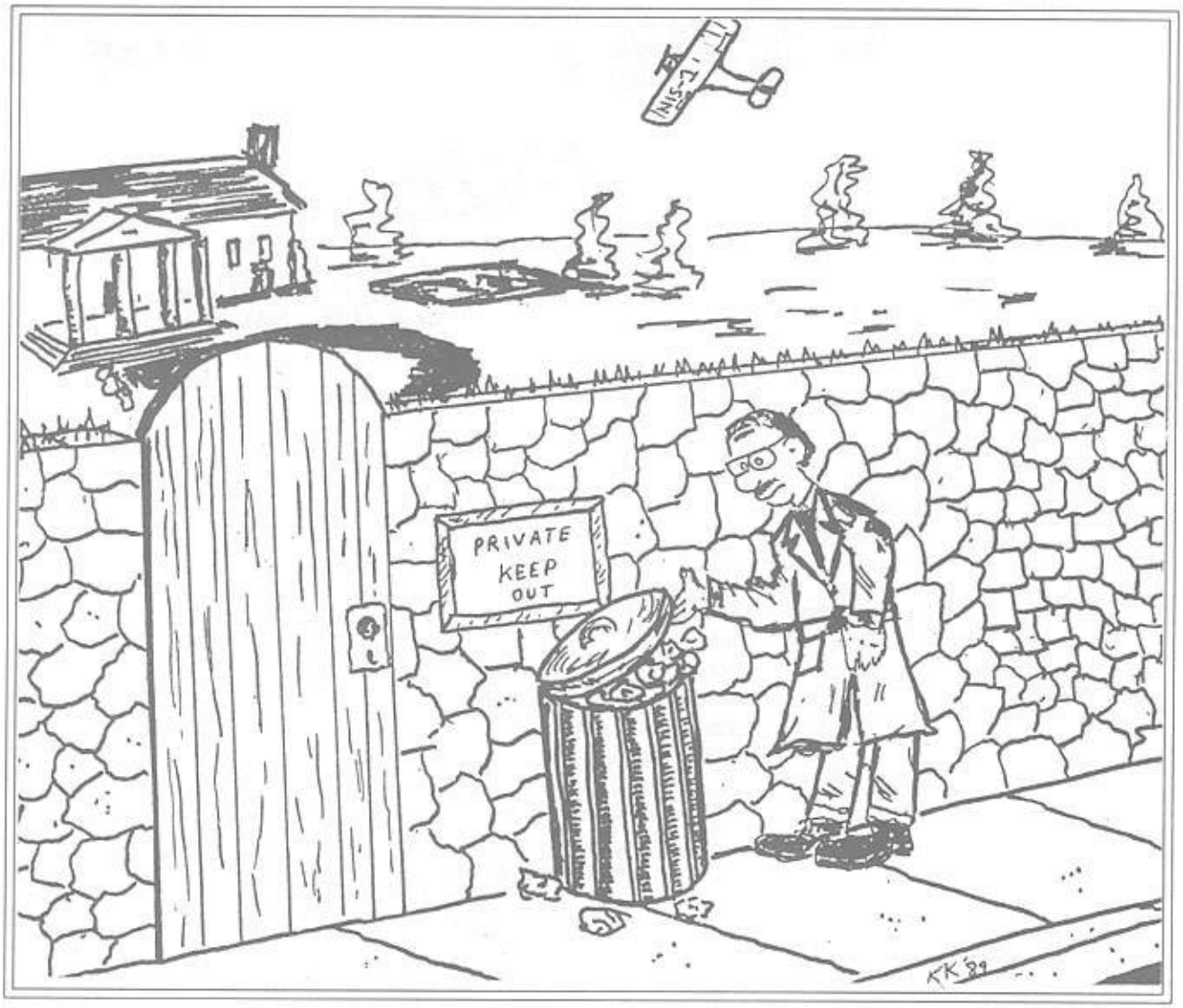
The Court noted that the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of society. By exposing his garbage to the public, the defendant gave up any reasonable expectation of privacy for its contents.

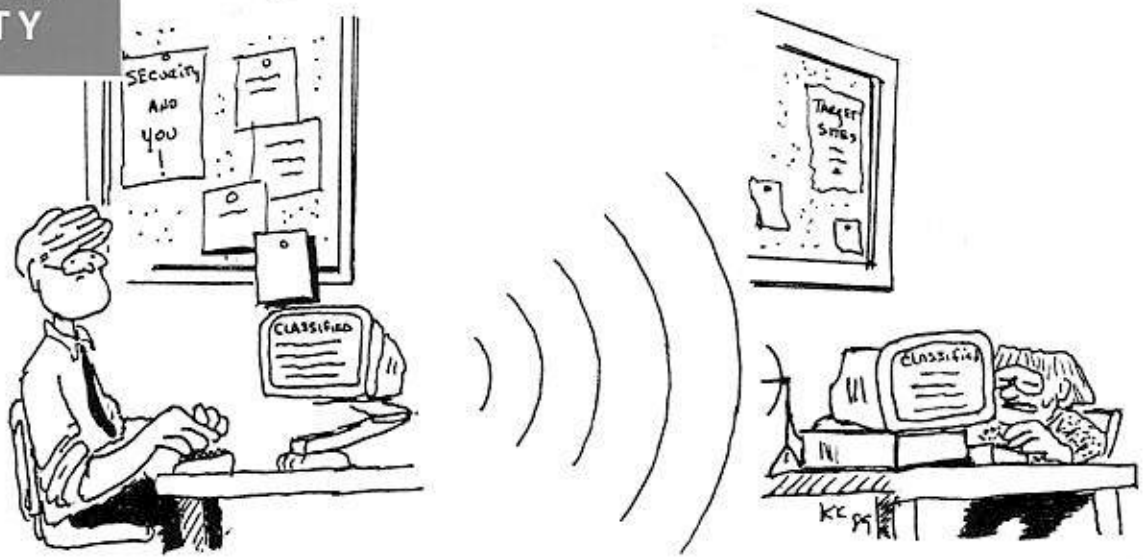
In another case, California v. Ciraolo, 476 U.S. 207, 211 (1986) a defendent had built a 10-foot privacy fence around his home to conceal marijuana plants. Police, suspecting that he was growing marijuana, flew over his yard in a chartered private plane and were able to see the plants with the naked eye. The Supreme Court ruled that the police overflight did not intrude into the defendant's privacy any more than that of an occasional civilian casually observing his

yard from a private plane, thereby removing any "reasonable" expectation of privacy. Since the police acted in the same manner as any member of the flying public could have and the defendant had failed to take measures to prevent a casual observance from the air, their "search" did not violate any legitimate expectation of privacy, and was legal.

The absence of "legitimate" expectations of privacy means that investigative activities do not violate the Fourth Amendment and the normal pre-requisites for a search -- probable cause, reasonable suspicion or search warrants -- are not required.

If the public has access -- so do the police! ★





TEMPEST - The INVISIBLE security threat

The requirements and responsibilities of the Navy Instrumented TEMPEST Program

by Michael I. Dunnington
Head, NISCOM TEMPEST Division

As a Navy manager you may get involved in purchasing an Automated Data Processing or other electronic system to process classified information. As managers, we are mainly concerned with ensuring funding is available and that the contracts are in place. However, there is a greater responsibility -- to system security.

While most security concerns occur after the purchase of equipment, security for electronic processors of classified information must be considered prior to even ordering it.

Electronic equipment, by nature, gives out unintentional emanations. These signals, known as Compromising Emanations or TEMPEST, if intercepted and analyzed, may disclose classified information transmitted, received, handled or otherwise processed by any information-processing equipment.

Navy implementation of the National Policy on the Control of Compromising Emanations is found in OPNAVINST C5510.93E dated 22 February 1988. This instruction applies to all activities of the Department of the Navy, Coast Guard and Navy contractors.

The directive implements, for the first time, an evaluation process, outlined in enclosure (3) of the instruction, that determines specific countermeasures that must be used in order to process classified information electronically. The evaluation takes into account command location, equipment used to process the classified information, and the level and volume of the information processed. Countermeasure evaluations are performed by the user command with the assistance of the command or local TEMPEST Control Officer.

After countermeasures are implemented and the equipment is purchased, the evaluation is attached as an enclosure to the TEMPEST Vul-

nerability Assessment Request.

This Request is required for all shore fix-plant or transportable classified information processors (specific exclusions are listed in the instruction), and is used to determine whether or not an Instrumented TEMPEST Survey is required. TEMPEST Vulnerability Assessment Requests, in letter format, should be submitted to Commander, Naval Investigative Service Command, Code 0026T, Washington, DC 20388-5000, and must contain information outlined in enclosure (4) of the instruction. (COMNISCOM is the Executive Agent for CNO TEMPEST Policy.)

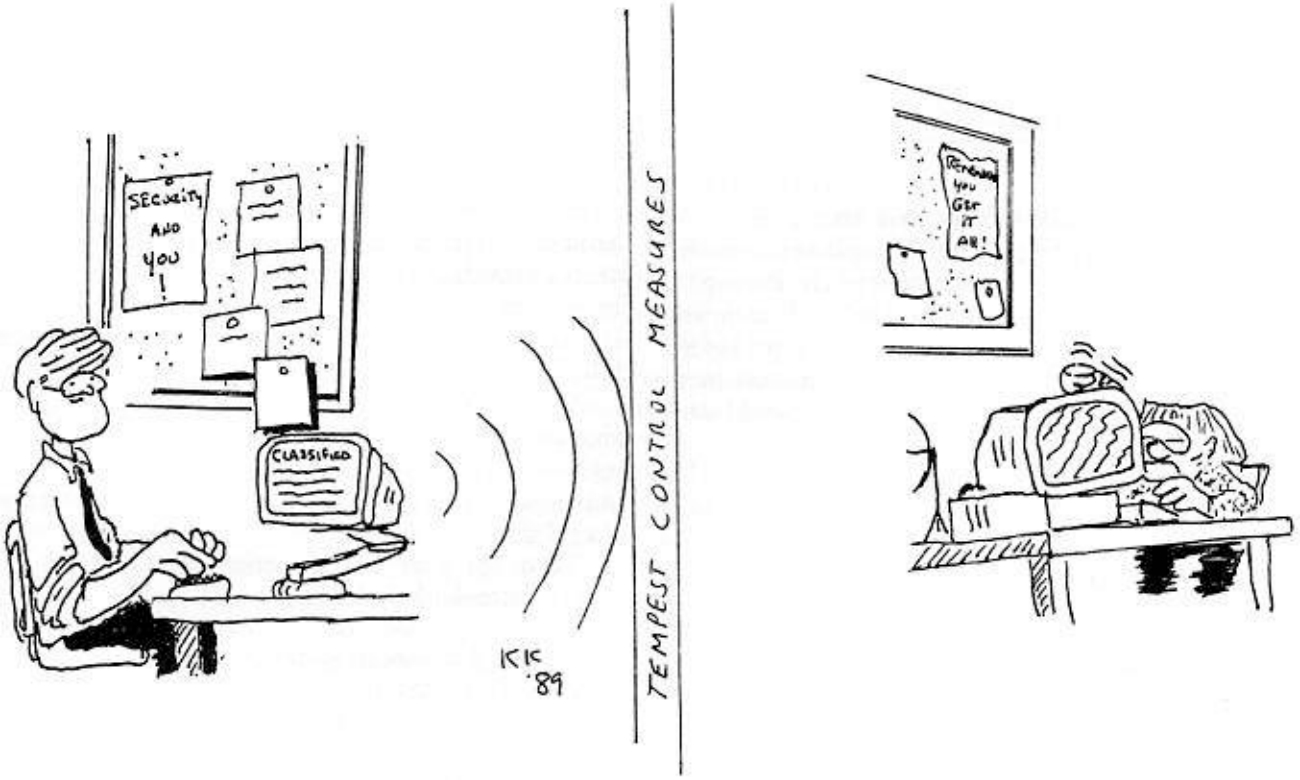
Navy TEMPEST policy for ships, aircraft and prototype systems are also outlined in enclosure (4).

OPNAVINST C5510.93E also implements the Navy TEMPEST Control Officer Program for the Commandant of the Marine Corps, the Chief of Naval Operations, and second echelon commands. These commands are required to designate a TEMPEST Control Officer at the headquarters level; however, it is recommended that TEMPEST Control Officers be designated at all command levels. By having these individuals designated at the facility or station level, the command ensures a detailed knowledge of all classified information processors under their responsibility.

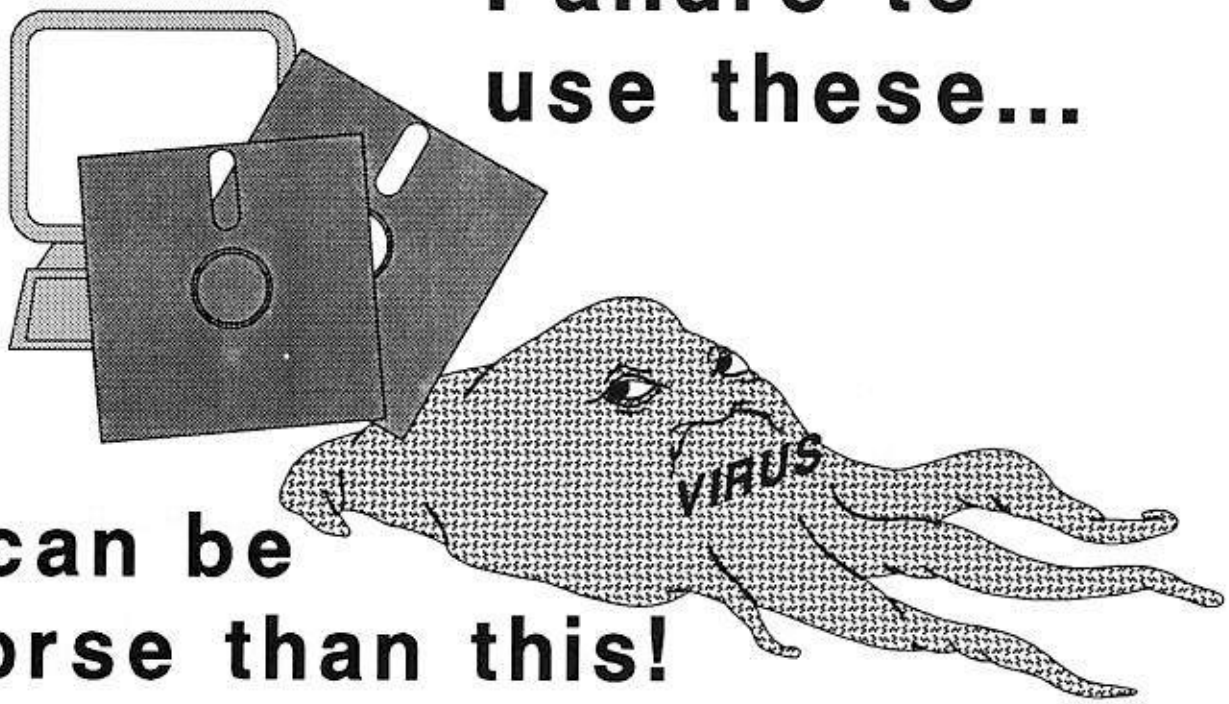
TEMPEST Control Officers assist equipment users in the performance of countermeasures evaluations, coordinate TEMPEST Vulnerability Assessment Requests, and maintain a library of TEMPEST-related documents. They also ensure the command implements TEMPEST requirements and conducts periodic checks for compliance, and maintains an awareness of all new procurement, development, or installation programs, ensuring that TEMPEST input or support is obtained.

TEMPEST security is not just the concern of a chosen few. TEMPEST Control Officers and TEMPEST Program Managers cannot do their job without the cooperation and vigilence of day-to-day equipment users. It is the responsibility of all those who process classified data electronically.

(Copies of the instruction may be obtained from the Navy Publications and Forms Center, Philadelphia, PA. Stock number is 0690-LP-001-0920.) ★



Failure to use these...



...can be worse than this!

How can you avoid the devastating effects of the loss of critical computer data? A good back-up system can save the day!

by Jerry T. Oney
Asst. Director, NISCOM Information Systems

The last several months have seen a number of articles in newspapers and magazines describing the dangers of computer viruses and the need to vaccinate our equipment against the AIDS of the computer world. These stories make for spectacular copy, but the actual threat posed to individual microcomputers by viruses is fairly negligible, especially in comparison to other threats.

In truth, more damage is done to computers by leaking roofs and clumsy-fingered Personal Computer (PC) users than by all viruses, worms, trojan horses, trap doors and logic bombs combined!

Based upon observations, the most overwhelming PC security problem is the loss of critical data due to inadequate back-ups. The major culprit in most fiascos is the internal hard disk -- the famous "C" drive. All of us learn a hard lesson when we inadvertently format the "C" drive or experience a hard disk failure that results in the loss of critical data. For many of us its like the first visit to the woodshed with Dad -- after the first trip, there is a great desire to avoid the same fate again.

For a variety of reasons, users do not learn to make back-up copies of even their most critical files. The process of copying large hard disk files to multiple floppy diskettes can be exceptionally frustrating. Under the best of circumstances, copying 20 megabytes of data to a large number of floppies can be very time consuming.

Because of its convenience, the hard disk has made it difficult to develop a good back-up habit until it is too late.

We all tend to believe "it can't happen to me," but when disaster strikes and we spend several hours explaining how it happened to our supervisors, reprogramming and re-creating files, then data back-up assumes the status of a religion.

There are a number of tactics you can employ to develop better back-up habits.

TACTIC 1 -- *Be aware of the threats against your system.* Shown at Figure (1) is the one-minute manager's guide to information security threats. All items are a threat against you; however, items 3-6 can be prevented by establishing good back-up techniques.

Analysis of the causes of Computer Data Loss	NATURAL AND NON-MALICIOUS ACTION	MALICIOUS ACTION
DATA DAMAGE	1. DISASTER	2. VANDALISM
DATA MODIFICATION (RANDOM)	3. MISTAKES	4. PRANKS
DATA DESTRUCTION	5. ERASURE	6. SABOTAGE
DATA MODIFICATION (SYSTEMATIC)	7. INCOMPETENCE	8. FRAUD
DATA DISCLOSURE	9. EXPOSURE	10. THEFT

(Figure 1)

TACTIC 2 -- ***Attend a class on back-up management procedures***. Everyone who uses a PC should attend back-up management procedure training. Back-up training should cover the use of both hard and floppy disk systems and provide instructions on how to back up and store programs and data via streaming tape and floppy diskettes.

TACTIC 3 -- ***Use a streaming tape to back-up your data***. If your computer configuration includes a hard disk, it should also include a streaming tape unit. If it doesn't, then acquire one at the earliest opportunity. Back-up to a streaming tape on a daily basis, alternating days with a minimum of two tapes.

TACTIC 4 -- ***Assess values to data to be protected and develop a system accordingly***. The importance of your data can normally be grouped into three categories and backed-up accordingly on floppy disks.

A. **Scratch-Pad Data**. This data is not important to your operation and there is no concern with losing it. Make a back-up copy on a weekly basis.

B. **Important Data**. This data is important, but not critical to your operation. Make two back-up copies and an archive copy. Make back-ups on Tuesday and Thursday, labelling the disks accordingly. Make the archive copy once a week and store it in another location.

C. **Critical Data**. This data is critical to the success of your operation and without it you would not be able to accomplish your mission. Make daily back-ups and a weekly archive copy.

TACTIC 5 -- ***Supervisors should perform periodic back-up procedure audits***. PC security and data back-ups are a management responsibility. When was the last time your supervisor checked your back-up procedures?

If microcomputer users and their supervisors employ these common-sense tactics, we may be able to accept an optimistic view of the PC world, and avoid Murphy's law.

Until these tactics are widespread, however, a large number of us are doomed to a trip to the woodshed. ★

Security classification labels for ADP media

by M. F. Brown, Head,
NISCOM Information Security Division

A recent OPNAVNOTE directed that Standard Forms 706 through 711 be used for security labelling on floppy disks, cassettes, cartridge disks, reel tapes, Winchester disks, microforms and other ADP media.

As commands began using the labels, these questions arose:

Q: *Do the labels fit on 3 1/2" diskettes? Does their placement interfere with the operation of the diskette in the computer system?*

A: The labels fit on the 3 1/2" as well as the 5 1/4" and 8" disks. However, care must be used to avoid interfering with their operation.

Q: *When should the SF-710, UNCLASSIFIED label be used?*

A: The SF-710, UNCLASSIFIED label is to be used only when both classified and unclassified material is processed in the same area. Its purpose is to help differentiate ADP storage media that do not contain classified information from those that do. In a space where all work is unclassified, the labels serve no purpose.

Q: *Can color codes and/or prestamped diskettes and other media be used without seeking a waiver?*

A: A waiver is necessary only when using alternative labels. The use of color coded (blue for CONFIDENTIAL, red for SECRET and orange for TOP SECRET) and/or prestamped diskettes is permitted without prior approval.

Q: *Are "Classified By" and "Declassify on" labels needed on ADP media?*

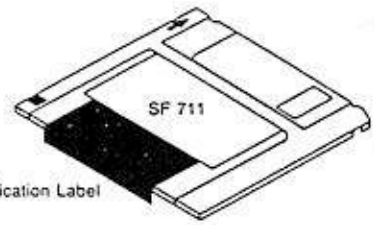
A: No, such labels would serve little purpose, since that information is subject to constant change depending upon the use of the media. ★

Optional SF 711 label placement
(When manufacturer's label is necessary)

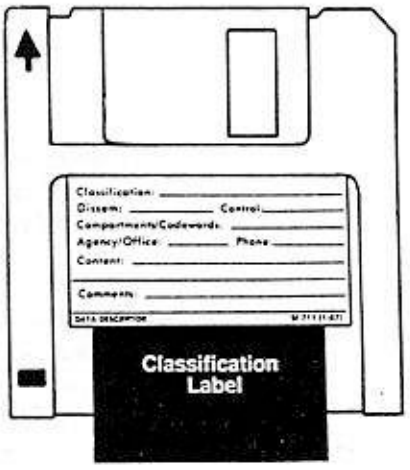
Suggested label placement
Always place the classification level label at the top of the diskette.

Exhibit A - 5-¼" Diskette
Place the SF 711, Data Descriptor label, on the upper left hand corner of the diskette, approximately 1/8 inch from each edge. Within approximately 1/8 inch from the right edge of the SF 711, place the appropriate classification level label, either SF 706, SF 707, SF 708, SF 709, or SF 710. Be careful not to place the classification level too close to the right edge of the diskette. If a manufacturer's label is already in the upper left or right hand corner of the diskette and the information on that label is necessary, place the SF 711 on the side of the diskette, as shown in the cut-out. The classification level label must remain either on the upper left or right hand corner of the diskette.

Exhibit B - 3-½" Diskette
Place the top edge of the SF 711, Data Descriptor label, at the top of the indented portion of the diskette. (This is on the side of the diskette without the hub.) Place the appropriate classification level label, SF 706, SF 707, SF 708, SF 709, or SF 710, directly below the SF 711. Press the bottom of the classification level label around the bottom edge of the diskette, so that the bottom edge of the label adheres to the side of the diskette with the hub. (When the diskette is placed in the computer's disk drive, you will be able to see the label color if the edge of the diskette protrudes.)



Fold and wrap the classification label around the bottom edge of the diskette.



In the Spotlight...

MACS James A. King

Counterterrorism 'expert'

by Barb Conrardy
Public Affairs Officer, Naval Air Station Barbers Point, Hawaii

When you want to know about something, the best source is an expert in the field.

When you want to know something about counter-terrorism, one such expert is Senior Chief Master-at-Arms James A. King.

King, a veteran of over 21 years in law enforcement, is the Command Senior Chief at Naval Air Facility, Midway Island. He has been studying terrorism since his tour of combat with the U.S. Army Special Forces in Vietnam from 1968 to 1971.

"We called it guerrilla warfare and insurgency back then," King said. "But it was terrorism in its purest form." King said he became interested in terrorism after seeing the effects of terrorism in combat, and seeing the effects in Europe.

"It seemed as if no one in the United States was interested," King said. "(Terrorism) was something that happened in Europe or Asia -- it doesn't happen here. But, of course, it can at any time." So King began studying terrorism and its effects.

During a recent assignment to Naval Air Station Miramar, California, King developed a curriculum for its Crisis Response Force training.

He taught a graduate-level course on Terrorism and Hostage Response at San Diego's National University, and wrote his doctoral dissertation on terrorism.

King has an impressive library of books on terrorism, including two he wrote, "Terrorism: A Practical Guide for Police" and "Providing Protective Services for VIP Protective Details." The books, published on 30 October 1988, are nestled among a large collection of video tapes and about 400 slides on the subject.

As a member of the National Tactical Officers Association, a nationwide police organization for special tactical forces, King recently had an opportunity to take part in a tour of Europe's top counter-terrorist teams that included a special unit of the Israeli Border Police, the French GIGN, Germany's GSG-9, and the Special Weapons Unit D-11 of the London Metropolitan Police. King also went through the diplomatic security driving course taught by the German Bundeskriminalamt -- the BKA -- an organizational equivalent of the FBI and the Secret Service combined.

"Driving a Mercedes-Benz at 85 miles per hour, on wet pavement, and then slamming on the brakes, is like an 'E' ticket ride at Disneyland," King said.

But all joking aside, King said the culmination of his 21-year law enforcement career came when he was given a birthday dinner in the special functions room at Scotland Yard.

He said he had made lots of friends on the security training trip, including the Deputy Commander of GSG-9, who was recently King's guest in San Diego.

King also said he especially enjoyed watching the changing of the guard from inside Buckingham Palace.

Because of his extensive background in the field, King is uniquely qualified to teach counter-terrorism, among other subjects. Besides his graduate degree, he also holds a California state teaching credential, and was awarded the title of Master Training Specialist while assigned as an instructor at Master-at-Arms Afloat and Shore Patrol School, Fleet Training Center, San Diego.

King is a certified PR-24 police baton and firearms instructor by the U.S. Navy and the State of California, and as a defensive tactics instructor by the FBI.

King was recently rewarded for his efforts in the training of crisis response and auxiliary security force personnel with a Navy Achievement Medal. ★

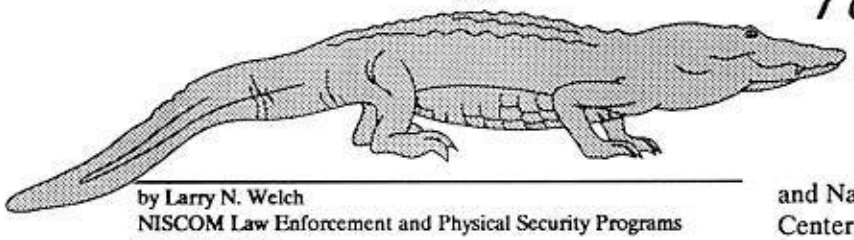
SECURITY OFFICER

In the Spotlight...

Dick Mulhare, NAVSECSTA

'Alligator Muldoon'

Top-notch security officer, programs



by Larry N. Welch
NISCOM Law Enforcement and Physical Security Programs Staff Assistant

His employees affectionately refer to him as "Alligator Muldoon," the guy who wants to employ low-tech base defenses with the installation of a moat. Ironically, though, he is nothing like America's answer to "Crocodile Dundee" and the security of his base is very high tech, in fact, it's a model.

"Alligator," whose real name is Dick Mulhare, is the security officer for one of the Navy's more unique installations -- Naval Security Station (NAVSECSTA).

One factor which makes this station unique is an unusually high degree of harmony and support between the major claimant, commanding officer, security officer, and security department employees. But it's the installation's location that presents some of the more unusual challenges.

Located in the prestigious Northwest suburbs of Washington, DC, the station's 38-acre site is surrounded by such neighbors as the Ambassadors from Sweden and Japan, the American University campus, an NBC-affiliate radio and television station, and The National Presbyterian Church. NAVSECSTA occupies the highest elevation in Washington, DC, but less than one mile away is the newly constructed Soviet Embassy. With a rooftop of antennas, the Soviet's are sited on an elevation near equal to the station -- convenient for electronic eavesdropping.

> *We operate a 'fair and friendly security service'*
> *– Dick Mulhare, NAVSECSTA*

As host installation to the Headquarters of Naval Security Group Command, Naval Telecommunications Command, Communication Security Material System, and Naval Electronics Systems Security Engineering Center, security for the station must be as flawless as humanly possible. Although Mulhare uses both Federal Service and Contract Guards, he far extends the human factor with over 200 Electronic Security Systems which are literally everywhere.

Included in his state-of-the-art defenses are electronic "sniffers" to check for explosives, X-ray screening systems for the mailroom and visitor centers, CCTV surveillance and anti-intrusion infra-red motion detectors, and conventional Intrusion Detection Systems (IDS) on fences, windows and doors.

It is a matter of pride to Mulhare that NAVSECSTA's electronic defenses have kept pace with technology. He recalled that upon arriving at the station in 1963, "...all we had were burglary alarms on doors -- that was the extent of our IDS. And now with the strong support of the commanding officer and our major claimant, COMNAVSECGRU, we are in a position where we can point to an integrated physical security/ antiterrorism defense which is model."

In addition to electronic security assistance, Mulhare has worked closely with public works for design and installation of less sophisticated, but no less important, automatic antiterrorist vehicle barrier systems, bullet-resistant shields in the guard and visitor's centers, and high-security lighting.

With 1,300 employees working in 20 buildings, Mulhare's small internal security force of 29 Federal guards -- even with augmentation by external contract guards, could not possibly hope to provide reasonable controls on physical security without use of technology. Mulhare stressed that NAVSECSTA's Electronic Security Systems are 100% operational at all times.

"We have a very capable work group which maintains our systems in an ever-ready condition," Mulhare said. "I have been to many bases that use various electronic sensors but half their gear doesn't work."

Physical security operations for Mulhare and

"Alligator Muldoon," alias Dick Mulhare, and the sign-map of Naval Security Station's 38-acre site in Washington DC. Formerly the Mount Vernon Seminary, a school for girls established around 1910, security for the station's 20 buildings present unusual challenges. (U.S. Navy photo by Mr. Ray Humenik, NAVSECSTA)

NAVSECSTA have not always been smooth-sailing. Recounting the most difficult periods in his 25-year tenure, Mulhare solemnly recalled the 1977 conversion to a contract guard service and the subsequent loss of their Marine Guard Company. The Marine departure from security assignments at NAVSECSTA was part of a well-intentioned restructuring effort to better employ Marine assets.

"It was an emotional experience which was exacerbated by our forced default of three guard-service contracts for failure to meet specifications. This resulted in our use of NAVSECSTA's crisis response teams to fill gaps until new contracts could be negotiated." He added, "Contract guard performance is better now but we'd still prefer a Marine sentry manning our external guard posts."

Some of the problems mentioned by Mulhare are commonly shared concerns of others in security. He said, "We operate a 'fair and friendly security service' but it is always a challenge to sustain employee awareness for the need to closely control base access, perform vehicle inspections, and check briefcases." According to Mulhare, "...this is a difficulty which requires continuing effort to create and then maintain proper employee attitudes regarding the importance of security -- information as well as physical."

Over his 25 years in a security role at NAVSECSTA, Mulhare's success story is typical of stalwarts who persist in working hard toward professional growth, and possess the flexibility to change with the times. Reporting to the station as a Damage Controlman in 1963, within a relatively short time he married, turned in his seabag for civilian service and went on to spend eight years apprenticed in maintenance of security systems, high security vaults, locksmithing, and fire protection. This was followed by six years as deputy security officer before taking the Security Department helm in 1977. Since that time the security program has been rated as 'outstanding,' likewise Mulhare has been the recipient of outstanding achievement awards year after year.

Exceedingly modest, Mulhare again and again attributes his professional growth to supervisors and coworkers who patiently explained the nuances of technical security as well as such sound management principles as organizational behavior, budget processes and the importance of planning.

James A. O'Hara, formerly a security specialist with the Naval Security Group Command and now Director, Law Enforcement and Physical Security Programs on the CNO Staff, said, "I've known Dick Mulhare for thirteen years. Upon meeting him in 1975 it was my initial impression that, '...this guy is one of the best in the security business,' and if anything this opinion has been strengthened with the passage of time." O'Hara continued, "Mulhare is thoroughly professional regardless of the situation. He is an intelligent planner, fair supervisor, and totally dedicated to the security mission.

> ***'This guy is one of the best in the security business'***
> ***– James A. O'Hara, NISCOM-24***

I know of a no more capable security officer within DOD."

Reluctant to accept credit for the remarkable planning, organization and installation of high technology security equipment and unusually well-executed day-to-day routines, Mulhare sincerely defers praise everywhere except to his own skillful management. He prefers instead to highlight commanding officer and major claimant vision for ESS adaption and funding, and his team of professionals for maintaining an even keel on security training, equipment maintenance, and the myriad of other details associated with NAVSECSTA security duty.

(Continued on following page)

'Alligator' *(Continued from previous page)*

Although now gray at the temples Mulhare continues to draw on the street-smarts of his youth in Newark, New Jersey. Whether walking the fence line, watching contract builders pour cement at NAVSECSTA's new Sensitive Compartmented Information Facility, or overseeing the escort of a disgruntled employee off-base, his eyes are alert for the unexpected -- that something that is out-of-place, or just not right. When asked whether his attention to such details is a result of growing up in a tough Newark neighborhood or 25 years in security, he laughed but was noncommittal.

A former NAVSECSTA guard lieutenant underscored the professional leadership advocated by Mulhare. "I never worked for a more fair-minded supervisor. Mr. Mulhare was always a constant source of inspiration in the way he encouraged all of us to learn and grow, both personally and professionally," said Marshall Schenck, who worked on the NAVSECSTA force between 1977 and 1986. "It seemed he was always anticipating trouble and, with fair accuracy, had us prepared for the unexpected."

Speaking of anticipating the unexpected, Mulhare simply smiled slightly when asked about the "Alligator Muldoon" moat. He later disclosed that members of the neighborhood's conservative architectural control committee would probably find the idea an impossibility.

Something tells us, however, that if he really thought it would help the security of his installation, Mulhare would fight for a moat. ★

NAVSECSTA Commanding Officer, Cmdr. Jay Wilkinson, with members of the security department following the presentation of 1987 outstanding performance awards. (From left, back row) Ray Toone, Deputy Security Officer and Roy Parker, Destruction Technician. (Second row) Dick Mulhare, Security Officer; Ray Anania, Criminal Investigator; Thomas Hendry, Guard Captain; and Dale Jones, Technical Security Specialist. (Front row) Annie Swindler, Assistant Security Clerk; Cristine Brown, Security Administrator; Carolyn McCoy, Assistant Security Clerk; and Officer Francis Smalls. (U.S. Navy photo by Ray Humenik, NAVSECSTA)

Model Base Security Plan available at Echelon II level

by Lt. Ron Rusek
LEPS Assistance Team Atlantic

Do you have a Security Plan? Just as important -- is it complete and workable? All Naval activities are tasked by OPNAVINST 5530.14(series) with producing a unit security plan. The plan is to include day-to-day security operations as well as contingency plans for how the activity will defend against various adversities, including bomb threats, terrorist activities, etc. The key point is that the plan must be feasible.

The Law Enforcement and Physical Security (LEPS) Assistance Team Atlantic has developed a comprehensive model Base Security Plan that can be adapted to your installation. The model plan was developed at the request and with the assistance of CINCLANTFLT.

The detailed plan, patterned after a major shore installation, is intended for use by commands ranging from large shore stations to the smallest tenants. It is not a "fill in the blanks" document, since only you know what elements are essential for your particular environment, but is intended as a guide to assist you in producing your own security plan and complying with the directive.

The document has recently been made available to Echelon II commands. ★

The Compendium... *finally!*

A compilation of reference and training materials for law enforcement and security programs

by Robert R. Bozzelli
NISCOM Antiterrorism Doctrine & Tactics Branch

Navy law enforcement and security professionals in the field have long expressed their concern regarding the absence of information on training and reference materials in the areas of law enforcement, physical security, antiterrorism, low intensity conflict and crime prevention.

In answer to this need, the Chief of Naval Operations (OP-09N) and the Naval Investigative Service Command (NISCOM) have developed the Compendium of Reference Material, intended as a ready reference document for security officers on courses, films and publications available for career development and training in these areas.

The information contained in the Compendium does not, by inclusion, imply that the course, film or publication has been approved for use by each security department. Requests for course attendance or film use must be submitted through the appropriate chain of command.

The Compendium, expected to be out sometime in March, will be distributed to security officers Navy-wide, with updates planned annually.

Comments and recommendations concerning the quality of the courses, films or publications listed are invited. Additional entries, deletions or other contributions may be provided to Naval Investigative Service Command, Code 24X32, Attn: Robert R. Bozzelli, Washington, DC 20388-5024. ★

Finding fund$ for your security projects

by "Andy" Anderson and Jeff Ross
NISCOM Physical Security Plans and Assessments Division

If your activity needs an integrated security system to safeguard a critical readiness asset, how does that need become a reality?

Let's examine this hypothetical situation.

You have coordinated this need within your activity and it developed into a $175K OPN project for a turnkey contract to buy and install the integrated security system. This issue is ranked with other funding requirements at your activity in accordance with guidelines provided by the major claimant (e.g., CINCLANTFLT, CNET, NAVSEA, etc.) as part of establishing Navy program objectives. These issues are forwarded, through the chain of command, to your major claimant for consolidation with other resource requirements.

Each major claimant prepares a Program Objectives Memorandum (POM) submission, which includes their security requirements, and submits it to the appropriate resource sponsors within the office of the Chief of Naval Operations (CNO), such as OP-03 or OP-05.

Every security issue is also forwarded to us -- CNO (OP-09N) -- as assessment sponsor for physical security. We review security issues from all major claimants and develop a Baseline Assessment Memorandum (BAM) which we forward to each resource sponsor for funding consideration. Baseline assessments are estimates of program costs necessary to meet CNO goals and ensure development of a balanced and consistent program. In other words, we assess or present a "bill" to each resource sponsor for security "services" needed for the Five-Year Defense Program.

The resource sponsors then decide how much of that bill can be paid, in relation to their total program. They evaluate funding requirements from each major claimant and each assessment sponsor, and develop a Sponsor Program Proposal (SPP).

After an iterative adjustment process, each SPP is presented to the CNO and the Secretary of the Navy (SECNAV), where further adjustments are made.

Finally, the Navy POM is submitted to the Secretary of Defense (SECDEF), who recommends total Navy resource requirements within the parameters of SECDEF fiscal guidance.

Interestingly, the foregoing description has been simplified for the sake of space. To give you an idea of the complexity, the actual POM-90 guidance package consisted of 39 documents, some running up to 127 pages.

The following questions may come to mind.

What has happened to, and where is, your $175K security requirement -- especially as it relates to the overall Navy submission, which was approximately $101.6 billion for FY 1988?

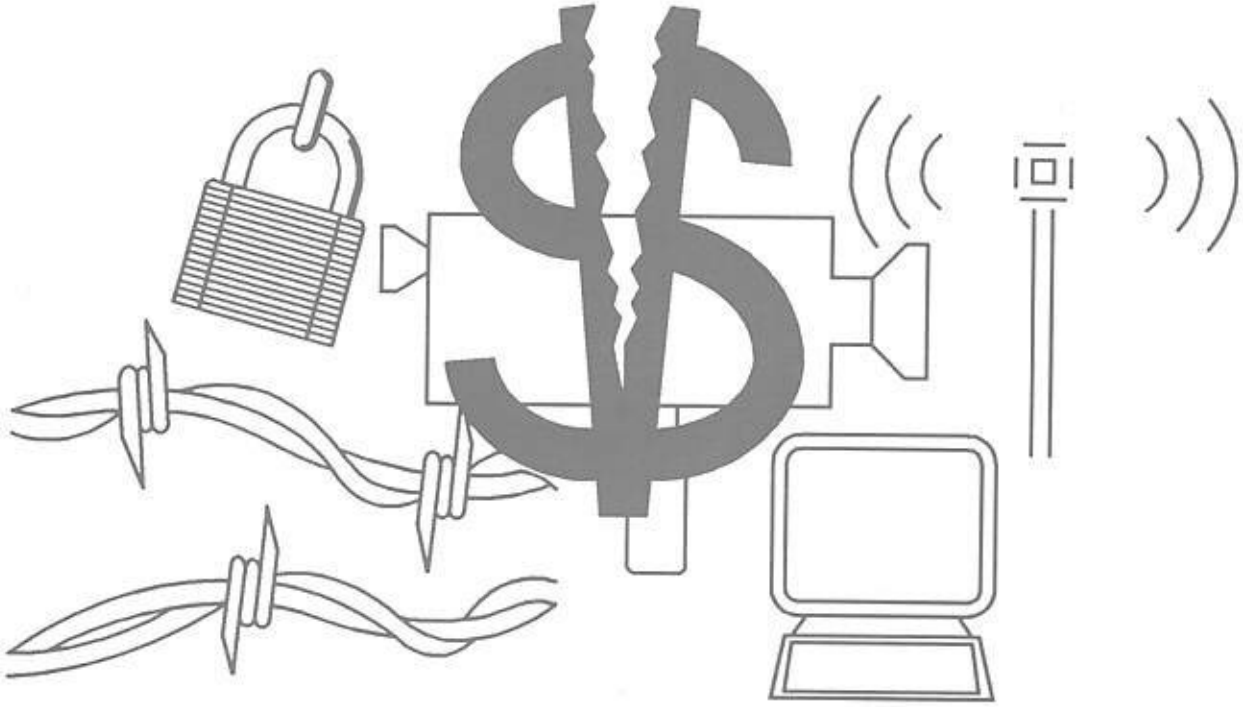
Does it still have visibility or identity in the overall perspective of Navy Maritime Strategy?

Can we, OP-09N, help you maintain a voice on the OPNAV staff?

How can we work together to support your requirements in the POM process?

First, a little more explanation of the process.

The number of issues that claimants may include in their POM submission is not limited; however, resource sponsors are only required to formally respond to the claimant's top five issues. Therefore, if a major claimant addresses security, and the need to safeguard their existing critical readiness assets as one of its top five issues, the resource sponsor will give more support to our security assessment. If the resource sponsor does not support it after it has been identified in the top five, we have an opportunity to address it in a post SPP Program Assessment "Heads-up" Report. In this, we summarize what



we consider to be significant funding deficiencies.

For the major claimant to address security as one of its top five issues, each activity should also rank security as one of its top priorities. For this to occur, it is critical that (1) detailed information/documentation is provided to support each project, and (2) the activity's commanding officer believes security is a high priority.

Here's where we can help. We have a limited staff that can, at your request and our expense, review, evaluate and assist in the preparation of physical security/anti-terrorism requirements prior to your submission to your claimant. Also, we can, and do, work with your major claimant to determine the best spread of available security resources.

The Navy has two principal and distinct peacetime responsibilities: (1) to maintain current fleet readiness, and (2) to ensure future force capabilities. To ensure Navy capability and readiness, we must have a commensurate program to safeguard critical assets and personnel who perform our crucial defense mission.

As an assessment sponsor, OP-09N has two basic tasks: (1) to identify long and short-term programming actions to achieve security levels necessary to accomplish the two principal Navy responsibilities, and (2) to assess the degree to which this is accomplished in the POM.

In other words, we <u>can</u> be your voice on the OPNAV staff as the security conscience of the Navy, and support the programs you need to the resource sponsors. We can aid your project development and support your requirements.

By the way, if you're wondering what happened to your $175K security requirement, it was approved, but the money has disappeared into the bulk of the appropriation. It is now up to the major claimant, the type commander, or the activity to program those funds during budget execution to support what was requested. ★

Security Communications (Part 2)

Definitions

by Michael J. Peebles
NAVELEX Charleston, Systems Engineering Division

Common terms used when describing communications systems are sometimes confusing to personnel not trained in this area. A clear definition of some of these terms can provide a better understanding of the land-mobile communications system used at your activity. The following is a alphabetical listing of definitions containing some of the more common terms used in communications.

Base Station -- A permanently installed **transceiver** at a fixed location. Most base stations have a much greater power output than other equipment in the communications system. Antennas for base stations are high gain and most often located on the highest point available. Controls for base stations can be located on the transceiver itself or controlled remotely (**remote control**) depending on the type of equipment.

DES - Data Encryption System. DES is algorithm developed by IBM for the National Bureau of Standards. It has been approved by the National Security Agency for the encryption of unclassified but sensitive national security related information. (A full article on DES will appear in the next issue of Sentry.)

Duplex - A communications channel which has separate transmit and receive paths. Duplex land-mobile communications channels have separate frequencies for these operations. Duplex channels must use a **repeater**.

Frequency Allocation - The authorization to use a specific type of equipment in a particular band of frequencies. All communications equipment must have a frequency allocation prior to procurement and **frequency assignment**.

Frequency Assignment - The assignment of a particular frequency for use within a specific geographic operating area using designated **transceiver** equipment. Although some frequencies for certain operations are assigned on a nation-wide or world-wide basis (such as maritime frequencies), most are authorized for use in only one geographic area.

Gain - The magnification power of the transmitted or received signal by the antenna. The gain of an antenna is usually measured in decibels or dB.

Remote **Control** - A piece of equipment which allows the control of functions such as volume, **squelch**, and channel selection, from a outlying location from the **transceiver** (similar to that of a TV remote you may use at home). This allows the **transceiver** to be located much closer to the antenna, which is a great advantage technically.

RF - Radio frequency.

Repeater - A piece of communications equipment which allows a single channel to transmit on one frequency and receive on another. The primary purpose of a repeater is to extend the range of a communications system by receiving information and re-transmitting (or 'repeating') it at greater power for extended range. The use of repeaters is especially effective in systems using hand-held radios which must operate over a large area. A hand-held radio is low-power and has limited range when talking to another hand-held on **simplex** channels. If a hand-held is within range of a repeater and operating on a **duplex** channel, the effective range of the radio is the same as the repeater itself and is greatly increased.

Simplex - A communications channel with the same transmit and receive path. Simplex land-mobile communications channels use a single frequency. Equipment operating on simplex channels talk directly to other units without benefit of a **repeater**, and usually have less range than **duplex** channels.

Squelch - An electronics circuit which turns off (or 'squelches') the volume when only noise is being received, the received signal level is very weak, or a specific series of tones is not received (between transmissions in tone-coded systems). There are two types of squelch: carrier and tone-coded. Carrier squelch operates based upon the received signal level regardless of the type of signal. Tone-coded squelch only turns on or unsquelches the volume when a specific series of tones is received. All **transceivers** in systems with tone-coded squelch generate these tones with every transmission.

Talk-around - A **simplex** channel which uses one of the frequencies of a **duplex** channel, thus bypassing the **repeater**. The talk-around channel permits communications to continue, with reduced range, if the **repeater** is disabled. Without the **repeater**, the **duplex** channel cannot be used and communications is impeded, unless a **simplex** channel is available. All systems containing a **repeater** should be designed with a talk-around channel.

Transceiver - Any piece of communications equipment which both transmits and receives signals. ★

THELMA THWARTUM — By Alex

A Public Service of AARP Criminal Justice Services

Fingerprint powder OK to use

Over the past four years, the Naval Investigative Service (NIS) has received many inquiries from the field concerning the potential health hazards of carbon black based fingerprint powders.

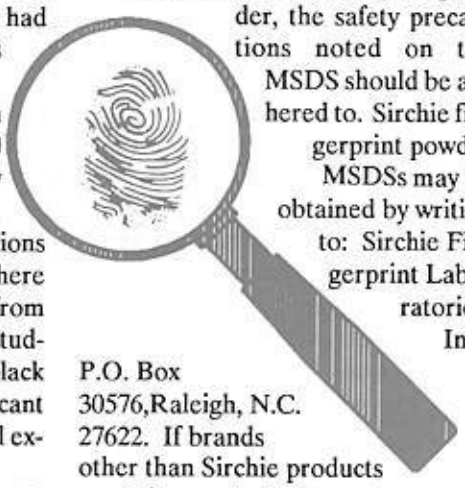
The charcoal in some powders of this type contained absorbed Polynuclear Aromatic Hydrocarbons (PNA), which was believed to cause lung and skin irritations, and possibly lung cancer.

One such powder specifically in question was the "Hi Fi Volcano" brand sold by Sirchie Laboratories, Inc., which is among the most commonly used brands in the Navy, and was found to contain the highest quantity of PNA hydrocarbons.

Contact with Sirchie Laboratories in June 1988 determined that as of 1985, the company has been using a carbon-based powder known as "Raven 1080 Black," which has had the hazardous PNA hydrocarbons removed.

The Material Safety Data Sheet (MSDS) for "Raven 1080 Black" states that the powder may cause temporary discomfort from inhalation of dust concentrations above permissable levels, but there are no recognized chronic effects from overexposure. Epidemiological studies of workers in the carbon black industry have shown no significant health effects due to occupational exposure.

From information currently available, carbon black based fingerprint powders produced after 1985, including Sirchie's "Hi Fi Volcano" brand, are considered safe to use. Although no evidence has proven any significant health hazards, pre-1986 "Hi Fi Volcano" brand fingerprint powders should be destroyed.



When using any fingerprint powder, the safety precautions noted on the MSDS should be adhered to. Sirchie fingerprint powder MSDSs may be obtained by writing to: Sirchie Fingerprint Laboratories, Inc., P.O. Box 30576, Raleigh, N.C. 27622. If brands other than Sirchie products are being used, the manufacturer should be contacted to obtain safety data sheets. ★

Reported by Maris J. Jaunakais
Head, NISCOM Forensic Sciences Division

Yes, Virginia. There really is a Navy Industrial Security Program

by Philip A. Bennett, Head,
NISCOM Industrial Security Policy

Those of you experiencing shortness of breath and rubbing your eyes in disbelief can rest assured -- there really *is* a Navy industrial security program.

In addition to information and personnel security policy, CNO (OP-O9N) is chartered with implementing the DOD Industrial Security Program (DISP) for the Navy. A full time position has been established with a mission to enforce DOD regulations in the Navy, render guidance and assistance, and address policy issues specific to our service.

We've been working hard to establish our presence within the Navy and industrial security community through close coordination with the Deputy Under Secretary of Defense (Policy) (DUSD(P)), the Defense Investigative Service (DIS) and major Navy procuring activities. Because industrial security involves all disciplines of security, the policy changes within the DOD security program forced us to do a lot of trench work to get things rolling again.

DOD/NAVY INDUSTRIAL SECURITY POLICY

The DISP is a system of requirements and procedures established to safeguard classified information entrusted to U.S. industry by the government. A contractor performing on classified contracts must implement these requirements with government advice, assistance and oversight. DIS administers the program with guidance from DUSD(P). They enforce the DISP and are the eyes and ears to industry for all User Agencies. (A User Agency is any federal department or agency that requires the services of contractors on a classified basis and subscribes to the policies of the DISP to acquire the services.)

DIS implements the DISP by publication of the "Industrial Security Regulation" (ISR), DOD 5220.22-R, and the "Industrial Security Manual for Safeguarding of Classified Information" (ISM), DOD 5220.22-M. The ISR establishes the program and sets the rules that User Agencies must follow. The ISM, on the other hand, provides industry with the rules and necessary guidance to properly safeguard government information. OP-09N currently implements the ISR within the Navy through publication of OPNAVINST 5540.8L of 27 June 1986. This directive addresses aspects of the DISP that are unique to the Navy and is the "operational" instruction for the Navy industrial security program. The instruction is presently going through a major revision that will be much more detailed, informative and readable. DIS expects to publish a revision of the ISR in early spring of 1989. We are aiming for publication of our revision to immediately follow that of the ISR. Keep an eye out for it!

INDUSTRIAL SECURITY TRAINING

It's a known fact that there is little or no awareness in the fleet about opportunities for training in industrial security. However, quality training is available!

The Department of Defense Security Institute, located at Defense General Supply Center in Richmond, Va., originally a part of DIS, is chartered with developing and presenting courses of instruction in all collateral security disciplines. Because of its roots with DIS, the Institute provides expert instruction in industrial security.

Two courses available are the "Industrial Security Basic Course", and the "User Agency Inspector Course". The basic course provides a general overview of the DISP through use of the ISR and the ISM and is the best explanation of industrial security available. If you are a contracting officer, security manager/specialist, or part of the security staff of a command involved in classified procurement, then this three-day course is highly recommended. The Inspector course provides security personnel with detailed instruction on recommended procedures for inspection of on-installation contractors. If your command is host to any contractor fa-

cility and your command has retained security cognizance over the contractor's site, then this week-long course is a must! (Don't be surprised if these courses become a requirement of our new directive for attendance by industrial security personnel of host commands.) Both courses are resident courses and are offered three times a year during a two week block. They can be taken separately from one year to the next or in a single block. Refer to exhibit 3E of OPNAVINST 5510.1H, Information and Personnel Security Manual, for descriptions of other security courses available.

Quotas for these courses are allocated to Navy commands by the Office of Civilian Personnel Management (OCPM). Inquire about quotas by calling OCPM at (202) 696-5097 or Autovon 226-5097. Despite the funding restraints we all face, security managers of host commands should make every effort to send industrial security personnel to these courses. At a minimum, security managers are encouraged to enroll their industrial security personnel in correspondence courses sponsored by the Institute.

"The Defense Industrial Security Program, Parts I and II" provides the student with a clear and easy-reading course on key topics within the DISP. Course catalogs and schedule updates are available from the Institute upon request by writing to: **Registrar, Department of Defense Security Institute, c/o Defense General Supply Center, Richmond, Va. 23974-5091**; or calling **(804) 275-4891** or AV: **695-4891.** ★

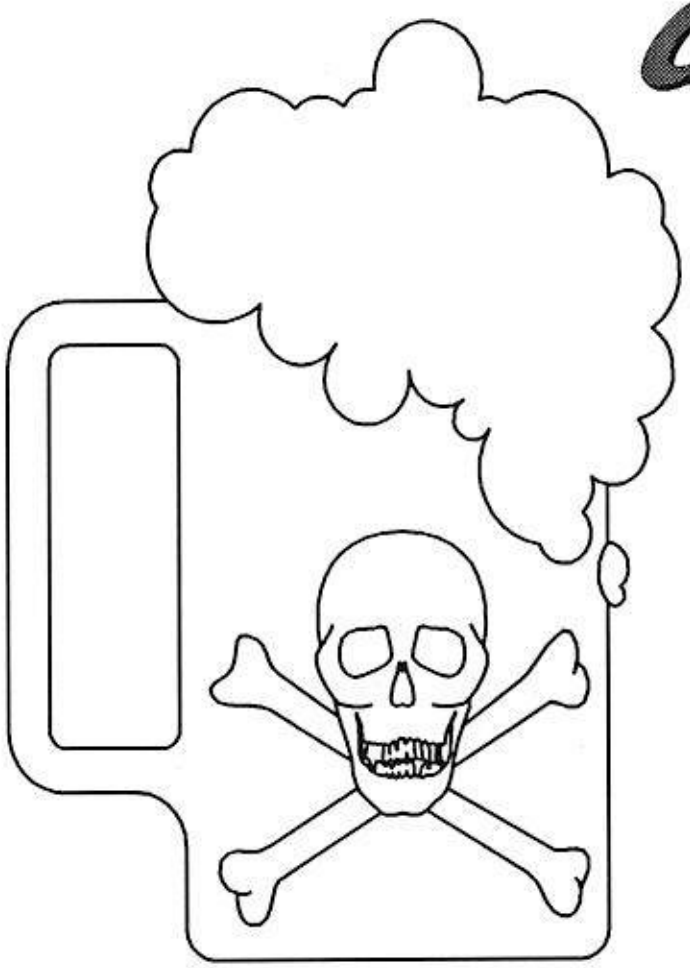
ATTENTION ALL HANDS, ATTENTION ALL HANDS!! DO NOT, I SAY AGAIN, DO NOT SEND CONFIDENTIAL INFORMATION VIA FIRST CLASS MAIL TO DOD CONTRACTORS OR NON-DOD AGENCIES

In the final issue of the *Information and Personnel Security Newsletter*, we alerted you to the increasing numbers of security discrepancy reports sent to us from the Defense Investigative Service concerning the use of First Class Mail by Navy activities when sending Confidential material to DOD contractors.

The reports keep coming in with no sign of slowing down. Paragraph 15-4.1c of OPNAVINST 5510.1H specifically states that you ***may not*** use First Class Mail to send Confidential material to a DOD contractor or non-DOD agency. The reason is that contractors and non-DOD agencies are not required to establish screening points to control incoming mail, thus access to classified information is not limited to cleared personnel only. The danger lies in that Confidential material sent First Class, may be opened by uncleared contractor employees working in the mail room.

Refer to paragraph 15-4 of OPNAVINST 5510.1H for the approved methods for transmission of Confidential information or call our **Security Action Hotline** at **(202) 433-8856** or AV: **288-8856**, and ask us! ★

Beer Drinkers' deadly myth



The brew often perceived as 'harmless' may be more hazardous to your health than wine or hard liquor!

Despite his hospitalization for severe stomach problems related to his drinking, George emphatically denied he was an alcoholic.

After all, he rationalized, his marriage was intact, he worked 40 hours a week and he was financially secure enough to drive a new car.

But George believed the strongest argument of all against his being an alcoholic was that he drank only beer. (No matter that he consumed two cases a day.) In fact, George had switched to beer believing that, no matter how much he drank, it was safer than the cocaine he'd been addicted to a year before.

George is not alone in assuming that beer is meant to be swigged by the mugful.

During 1981, the per capita consumption of beer in America was 26.6 gallons compared to 2.6 gallons of hard liquor and 2.4 gallons of wine.

Beer consumption may increase even more with the introduction of "instant beer" developed by Mostafa Hamdy, a University of Georgia researcher. Hamdy is seeking a patent for his product which is designed for "consumers who want a truly light beer to carry along on a hike or keep in the pantry to mix by the glassful."

The high rate at which Americans drink beer probably centers on the perception that beer is a relatively harmless beverage -- a view reinforced by the highly visible advertising campaigns sponsored by the competitive brewing industry.

Most of those ads portray beer drinkers as backslapping good ole' boys whose good, clean fun is enhanced by an ever-present, foaming mug of brew.

Some brewers even tout the healthfulness of their beverages. One Canadian study claimed that beer drinkers had fewer illnesses than teetotalers or those who drank other alcoholic beverages. The credibility of

that research suffers, however, considering that one of the study's sponsors was the Brewer's Association of Canada.

While it's true that, ounce for ounce, beer has less alcohol than equal amounts of wine or hard liquor, a more suitable comparison would be between typical serving sizes. In that respect, a 12-ounce can of beer, a four-ounce glass of wine and a one-ounce shot of whiskey have virtually the same amounts of alcohol.

Even so-called "light" or low-calorie beers contain almost as much alcohol as regular beer. While regular beers have alcohol contents ranging from 3.6 to 4.4 percent, light beers are 2.4 to 2.8 percent alcohol.

Research also indicates that beer may pose it's own unique health risks to those who drink it as their main alcoholic beverage of choice.

According to research conducted at six Veterans Administration hospitals, heavy beer drinkers apparently are at greater risk of dying of liver disease than people who abuse the same amounts of wine or hard liquor.

The study released last year found that the five-year survival rates from alcoholic hepatitis were only 24 percent for heavy beer drinkers, compared to 45 percent for those who abused hard liquor and 58 percent for those who drank mainly wine.

Studies also show that beer drinkers are more likely to drive while intoxicated than people who consume mainly hard liquor or wine. In a 1983 survey of 1,000 American drivers conducted by researchers at the Clairmont Colleges in Clairmont, California, more than half of those who drink primarily beer said they drove while drunk compared to 28 percent of wine drinkers and 31 percent of those who consume hard liquor.

As the dangers of beer drinking have been exposed, many people may be tempted to "go on the wagon" with so-called non-alcoholic beer, but they should be on guard, particularly if they are recovering alcoholics. Current federal regulations consider a beverage non-alcoholic if it contains less than 0.5 percent alcohol. While half a percent of alcohol is not a danger to the average drinker, it may be enough to cause the alcoholic to "slip" during recovery.

Chemical dependency experts also fear that non-alcoholic beer may cause relapse because it closely resembles beer and may encourage the alcoholic to revert to "the real thing."

★

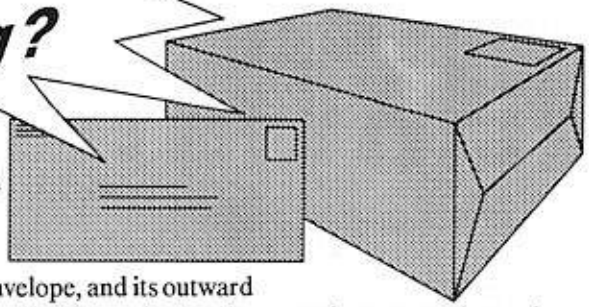
Reprinted from the July 29, 1988 edition of the Kings Bay Periscope, Naval Submarine Base, Kings Bay, Georgia.

Defending against terrorism

Part 6 in a series

by JO1 John S. Verrico
NISCOM Public Affairs Assistant

Mail Bomb! *Is it ticking?*



In Grants, New Mexico, the intended victim of a mail bomb was killed and another was seriously injured on October 24, 1988. A supply man at a local uranium mine, whose job included the distribution of gel-type explosives and blasting caps, was suspect. A task force of Postal Inspectors and personnel from the local Crime Laboratory determined that the man had brought the armed device aboard a commercial airliner as carry-on baggage and flew from Albuquerque, New Mexico to Las Vegas, where he mailed it to his intended victim. He was arrested and charged with homicide.

According to a report by the Chief Postal Inspector, this was only one of 10 mail-bomb incidents that occurred in the continental United States in a two-month period. In the other incidents the bombs had detonated in collection or mail boxes and no injuries were reported. Many of these devices were pipe bombs.

The likelihood that you will ever receive a bomb in the mail is remote, however, all too many of these devices have resulted in death, injury and destruction of property over the past few years.

What can you do to prevent a mail bomb disaster? Keep in mind that a bomb can be enclosed in either a parcel or an envelope, and its outward appearance is limited only by the imagination of the sender. However, mail bombs have exhibited some unique characteristics which may assist you in identifying suspect mail. To apply these factors, it is first important that you know the type of mail that you or your organization regularly receive.

Mail bombs may bear restricted endorsements such as "Personal" or "Private." This factor is important when the addressee does not normally receive personal mail at the office. Also, the addressee's name or title may be misspelled or otherwise inaccurate.

Mail bombs may bear distorted handwriting, or the name and address may be prepared with homemade labels or cut-and-paste lettering.

Watch for protruding wires, aluminum foil, or visible oil stains, and be alert for peculiar odors, like that of cleaning fluid or almonds. Mail with an excessive amount of postage stamps should also be suspect.

Letter bombs may feel rigid as cardboard or other stiffeners are used to hold spring-loaded devices. They may also appear uneven or lopsided.

Parcel bombs may make a buzzing, ticking or sloshing sound. They may be unprofessionally wrapped with several combinations of tape used to secure the package. Another aspect to watch for is an irregular shape, soft spots or bulges. Pressure or resistance should be noted when removing contents from an envelope or package.

Most importantly, if you have any reason to be suspicious about a mailing and are unable to identify the sender or verify the contents, do not open it!

Isolate the parcel or envelope and evacuate the immediate area. If possible, open nearby windows to assist in venting potentially explosive gases. Do not put it into a confined space such as a desk drawer or filing cabinet. If it is a bomb, and it goes off, you are only supplying it with additional shrapnel.

Don't try to take action on your own by placing it in water! Some chemical devices are water-activated.

Contact your local security or police department and Postal Inspector immediately. Don't worry about the possibility of embarrassment if the item turns about to be innocent -- ***don't take a chance!*** ★

From the U.S. Postal Inspector's Crime Prevention HOTSHEET "Bombs by Mail," and the Chief Postal Inspector's Postal Related Bomb/Explosive Incident Summary; September & October 1988.

Security Awareness Poster Contest deadline extended!

The deadline for the Security Awareness Poster Contest has been extended to 1 July 1989 and the prize is being upgraded.

Although only one winner will be selected, all entrants will receive recognition for their efforts. Entries will be judged on the Security Awareness concept of each poster, and not on the quality of the art. OP-09N2 will produce a poster, redrawn to professional standards if needed, based on the winning concept. Runners-up may also be selected for publication as posters.

All posters will become property of the Department of the Navy and, when published, will become public domain. For this reason, do not submit copyrighted materials.

Submit ***original*** ideas and/or artwork to: **Chief of Naval Operations (OP-09N2), Security Awareness Poster Contest, Naval Investigative Service Command (Code 21), Information and Personnel Security Policy, Washington, DC 20388-5021.** Refer questions to James McElroy at AV: 288-8855 or Comm: (202) 433-8855.

NIS Espionage Hotline

How's it going?

The Department of the Navy (DON) Espionage Hotline was established in May 1985 as an adjunct to the BOBSLED Task Force, a joint agency operation formed to investigate the espionage activities of Marine Sgt. Clayton Lonetree. Today, the hotline provides DON personnel direct, confidential access to the Naval Investigative Service (NIS) to report information that may be related to spying or security violations affecting the Navy or Marine Corps.

One of the most significant reports received through the hotline occurred in October 1987 when a Navy member reported the irregularities of a shipmate's handling of classified information. The subsequent NIS investigation led to the arrest and court-martial of a senior enlisted man for the unauthorized removal of highly classified information from his command.

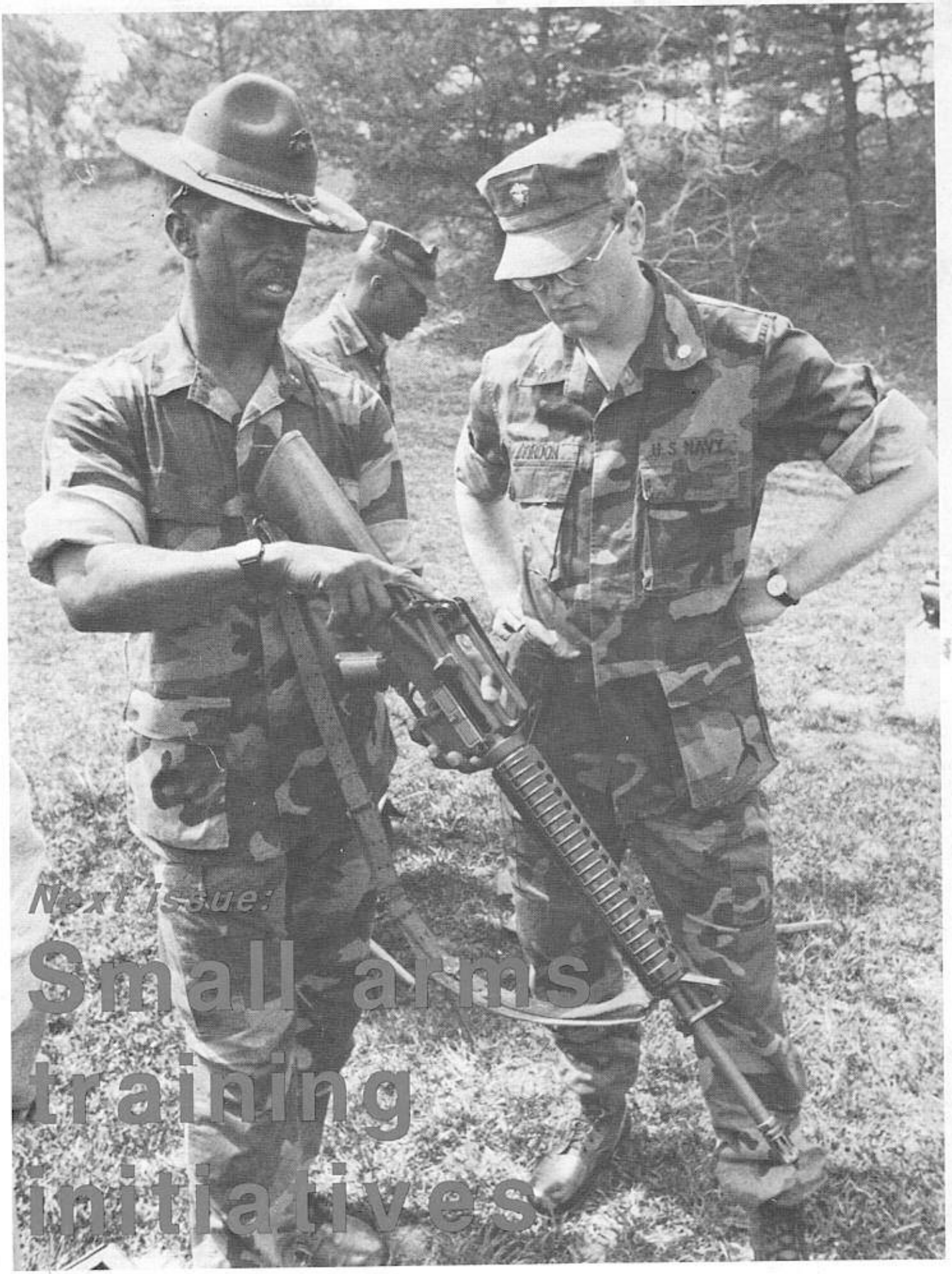
In January 1988, the hotline moved to the Naval Investigative Service Command (NISCOM) Counterintelligence Directorate at the headquarters in Washington DC. Since then the hotline has processed 39 calls, an average of three-four each month.

Approximately 85% of the calls received result in some type of investigative or administrative action by NIS. Those calls which provide sufficient information to initiate an investigation are forwarded to the nearest NIS Resident Agency.

The DON Espionage Hotline exists to give people in the fleet the means to report possible espionage or security violations while maintaining their confidentiality.

The call is toll-free, 1-800-445-7343, anywhere in the United States. Efforts to expand the use of the hotline, including the means to make the system available to overseas personnel, are in progress. ★

(800) 445-7343



Next issue:

Small arms training initiatives