

Info **DO**MAIN



Summer Edition 2013

- 2 My Domain**
NETWARCOM Commander speaks candidly about career & challenges.
- 10 Vulnerability Scan Required for Navy Website Health**
Responsibility for protection, content & compliance on websites lies with COs.
- 12 Cyber Cat Tips**
Protecting & Avoiding Becoming Victim of Ransomware.
- 18 Training For Nothing and the SMEs for Free . . . for Now**
NAVCYBERFOR's FAST workshop provides training for commands at no cost.
- 21 2nd Satellite to Boost DoD Satellite Communications**
Users are going to notice more bandwidth, better voice quality and connectivity.
- 23 Rescue Airmen Support Historic Rocket Launch**
Reserve Airmen from 920th Rescue Wing prevent incidents at launch time.
- 24 CIO's Network Tips**
Malware prevails if Sailors allow it.
- 26 Guide to Implementing Knowledge Management in a Stike Group Staff**
Commander shares insight and techniques to be used in a broader context.
- 29 Safari Books OnLine**
You name it – you can learn it OnLine & for free.

- 4 HqtrsCYBERFOR** **8 Short Circuits** **11 Cyber Warriors**
- 14 CID Spotlight** **31 Team Spotlight** **35 People Spotlight**
- 38 NMOC Spotlight** **42 Special Recognition** **48 Diversity**

FRONT COVER: *An Atlas V rocket launches the Navy's Mobile User Objective System (MUOS) 2 satellite from Space Launch Complex-41 at Cape Canaveral Air Force Station, FL. MUOS is a next-generation narrow band tactical satellite communications system designed to significantly improve beyond-line-of-sight communications for U.S. forces on the move. For more information on the launch see Pages 21-23. (Photo courtesy of NASA by Patrick H. Corkery)*



Commander, Navy Cyber Forces
RDML Gretchen Herbert

Deputy Commander
Mr. Mark E. Kosnik

Public Affairs Officer
CDR Matt Klee

Deputy PAO / Editor-in-Chief
Mr. George D. Bieber

Managing Editor
Miss Jacky Fisher

**Associate Editor &
Visual Information Specialist**
Mr. Robin D. Hicks

Graphics Editor
MC2(SW) Jacob D. Galito

InfoDomain is the professional magazine of Navy Cyber Forces that promotes the advancement of Information Dominance through an open exchange of better practices, tactics and current and future strategies to meet the global challenges of the information warfare domain.

Information contained in *InfoDomain* does not necessarily reflect the official views of the U.S. Government, the Department of Defense or the Department of the Navy. Editorial content is prepared by the Public Affairs Office of Navy Cyber Forces.

Articles for publication in *InfoDomain* should be submitted through the appropriate command representative. Security and policy review must be completed by submitting commands before submissions can be considered for publication. Address all correspondence to Editor in Chief, InfoDomain, Navy Cyber Forces, Public Affairs Office, Joint Expeditionary Base Little Creek - Fort Story, 2465 Guadalcanal Road, Suite 10, Virginia Beach, VA, 23459-3243; telephone (757) 417-7958 ext. 5, DSN 537-7958 ext. 5, FAX (757) 492-8702. Comments or queries may also be forwarded via e-mail to: george.bieber@navy.mil



Chandler Speaks Candidly About Career & Challenges

By MC1(IDW/SW/AW) Elizabeth Burke, NETWARCOM Staff Journalist

On Sept. 17, CAPT John W. Chandler will turn over the helm of the Naval Network Warfare Command (NETWARCOM) to CAPT Eugene D. Costello.

Chandler, a Monticello, AR, native received a nomination to the U. S. Naval Academy and was commissioned in 1987 with a degree in Physical Science.

Annapolis is a long way from Arkansas, so how does a young man from Arkansas get to the Naval Academy? Chandler was a competitive tennis player in high school and was being recruited by some big name schools for a tennis scholarship. Chandler was concerned that if he was to get injured he would lose the scholarship.

He had one other option. His father was a professor at the University of Arkansas at Monticello, and he could have lived at home and attended school there inexpensively, "But of course every kid wants to get out of their hometown," said Chandler.

He knew another Arkansan who attended the Naval Academy to play tennis so he wanted to do the same. Being from Arkansas was actually a bonus for Chandler because it is less competitive to apply for a Naval Academy nomination.

During his career which spanned almost three decades, Chandler's first operational tour was as the Combat Information Center Officer aboard USS Aubrey Fitch (FFG-34), where he earned his qualification as a Surface Warfare Officer (SWO). He then served as the Commander Destroyer Squadron SEVEN Assistant Operations Officer, participating

in Operation Desert Storm while embarked on USS Ranger (CV-61). During his next afloat operational tour, he completed his SWO department head tour as the Operations Officer on USS McInerney (FFG-8).

In 1999, two years prior to the establishment of the Information Professional (IP) Community, Chandler transitioned to a 1700 designator as a Space and Electronic Warfare Officer. "About 80 percent of the Space and Electronic Warfare officers became the plankowners of the IP Community," said Chandler. "We were at the beginning of it and then what the IP Community really did for us was give us a real career track, a real sea shore/rotation and meaningful afloat milestone jobs."

As an IP officer, he served in critical at-sea positions as Commander Cruiser Destroyer Group (COMCRUDESGRU)-12's Flag Communications Officer on USS Enterprise (CVN-65); as Command, Control, Communications, Computers, Combat Systems and Intelligence

(C5I) Officer on USS Nassau (LHA-4); and as Information Warfare Commander for the USS Theodore Roosevelt (CVN-71) Strike Group.

"I am not a hacker or a coder or anything like that but I have certainly always been interested in how technology would make almost any process or any job better," said Chandler.

Ashore, Chandler earned a Master of Science degree in Applied Physics at the Naval Postgraduate School in 1994. He completed assignments at the National Reconnaissance Office; on the staff of the Chief of Naval Operations; as the Operations Officer

"I'm not a hacker or a coder or anything like that but I have certainly always been interested in how technology would make almost any process or any job better."



Official U.S. Navy Photo

CAPT John W. Chandler

for Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT); and as the Knowledge Manager for U.S. Fleet Forces Command. He also served as the Commanding Officer of NCTAMS LANT from 2009 through 2011.

Assuming command of NETWARCOM on

... continued on Page 3





(Left) CAPT John W. Chandler, commanding officer Naval Network Warfare Command, shares a few laughs with RDML Gretchen Herbert, commander Navy Cyber Forces following a recent retirement ceremony. (Photo by Michael J. Morris)

(Right) CAPT John W. Chandler, commanding officer Naval Network Warfare Command, speaks at an Armed Forces Communication and Electronics Association (AFCEA), Hampton Roads Chapter luncheon, Aug. 13, 2013. (Photo by Michael J. Morris)



October 4, 2011, his three biggest challenges were transitioning the command from a flag command into an agile and tactical Task Force able to make quick Network Command and Control decisions; the preparation for the transition to the Next Generation Enterprise Network (NGEN); and the move of 350 personnel to the Navy Global Network Operations and Security Center in Suffolk, VA. “Those three huge tasks made for a very fast two years,” said Chandler.

The one thing that Chandler stressed about his tenure at NETWARCOM was the people. “I am

going to talk about this at the Change of Command quite a bit, just the level of expertise that exists at this command,” said Chandler. “What a service treasure we have here with lifelong communicators that have been served upward of 30 years in uniform and now ten to 15 years as civil servants and contractors, just being able to harness that knowledge and expertise has been awesome.”

Chandler’s plans for his follow on career are still tentative, but, “my intentions are to stay in the IT Management and Cyber Security Management field as a civilian,” Chandler said. “I love this field.” ✂

AT A **GLANCE**

CAPT John W. Chandler is a native of Monticello, AR. Chandler was commissioned in 1987 through the U.S. Naval Academy. He has been the Commander of Naval Network Warfare Command and Task Force 1010 since Oct. 4, 2011.

Chandler’s first operational tour was as the Combat Information Center Officer aboard USS AUBREY FITCH (FFG 34), where he earned his qualification as a Surface Warfare Officer. He then served as the COMDESRON SEVEN Assistant Operations Officer, participating in Operation DESERT STORM while embarked on USS RANGER (CV 61).

During his next afloat operational tour, he completed his SWO department head tour as the Operations Officer on USS McINERNEY (FFG 8). Following that tour, he laterally transferred into a new warfare designator - Information Professional (IP) - becoming a “plank owner” in the community.

As an IP officer, he served in critical at-sea positions as COMCRUDESGRU-12’s Flag Communications Officer on USS ENTERPRISE (CVN 65); as Command, Control, Communications, Computers, Combat Systems and Intelligence (C5I) Officer on USS NASSAU (LHA 4); and as Information Warfare Commander for the USS THEODORE ROOSEVELT (CVN 71) Strike Group.

Ashore, Chandler earned a Master of Science degree in Applied Physics at Naval Postgraduate School in 1994. He completed assignments at the National Reconnaissance Office; on the staff of the Chief of Naval Operations; as the Operations Officer for Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT); and as the Knowledge Manager for U.S. Fleet Forces Command. He also served as the Commanding Officer of NCTAMS LANT from 2009 through 2011. ✂

RECRUITING, TRAINING AND MAINTAINING TALENT IN THE CYBER WORKFORCE

By Sharon Anderson, SPAWARSCEN Atlantic

Today's cyberspace professionals can command high pay and the competition for their talents is fierce in all areas of industry, academia and government. While the need for cyber expertise is acute, the pool of qualified candidates is small, which presents a significant recruiting, training and retention challenge for the Department of the Navy (DON).

The DoN cyberspace/information technology (IT) workforce performs a broad range of mission-critical jobs: computer security; information assurance; network administration, analysis and defense; acquisition; and electromagnetic spectrum operations. The Navy's Information Dominance Corps (IDC) includes specialists in intelligence, information warfare, information operations, meteorology, oceanography and space communities and is comprised of 44,000 military (officer and enlisted) and civilian personnel.

At a military conference, three of the DON's cyberspace/IT leaders

tackled the difficult question of how to attract, train and keep individuals with these skill sets working in the Navy and Marine Corps as military and civilian cyberspace professionals. Ken Gill, the Assistant Chief of Staff G6 for Marine Forces Command; Terry Halvorsen, the DON Chief Information Officer (CIO); and RDML Gretchen Herbert, commander, Navy Cyber Forces, debated the topic in a panel discussion at the Joint Warfighting Conference in Virginia Beach, VA.

Gill said his concern for the Marine Corps is not in recruitment but in training and retaining cyberspace professionals. Typically, the Marine Corps loses a significant number of its military personnel annually. To compensate for the loss and as

"To attract and sustain a pool of cyberspace/IT professionals, the DON must develop creative ways to compete with salaries offered by the commercial sector."

Terry Halvorsen, DON CIO

it reshapes the force, since 1990, the Marine

Corps has been rebalancing the workforce through the revision of its Military Occupational Specialty (MOS) codes, including those dealing with cyberspace. The specialties encompass a system of categorizing career fields with corresponding training and job requirements. All enlisted and officer Marines are assigned a four-digit code denoting their occupational field and specialty.

Gill said the Marine Corps is moving

away from training in stovepipes and is leveraging cross-training opportunities. For example, network personnel will learn everything that is job related in their field, and will remain focused on the Marine Corps' core warfighting mission. Gill underscored that it is not just a matter of recruiting manpower but the right manning in filling cyber jobs.

Halvorsen agreed with the need

[... continued on Page 5](#)



(Center, left to right) Ken Gill, Asst. COS G6, Marine Forces Command; RDML Gretchen Herbert, commander, NAVCYBERFOR and Terry Halvorsen, DON CIO, discuss their answers with an audience at a Joint Warfare conference in Virginia Beach, VA. (Photo by Robin Hicks)



... continued from Page 4

for cross-training and said it will be necessary to blend the entire military and civilian cyberspace/IT workforce to meet critical gaps in manning.

“There will be a cultural shift in the department’s cyberspace/IT workforce planning and training efforts,” he said.

To attract and sustain a pool of cyberspace/IT professionals, the DON must develop creative ways to compete with salaries offered by the commercial sector. The department must make the case for and defend the resources necessary to support continuous training because technology and cyber threats change rapidly. According to Halverson, it will be necessary to create recruiting incentives and develop different compensation models and possibly special pay categories to fill critical gaps in cyberspace/IT positions.

To fill shortfalls in cyber manning, Herbert offered a unique approach that industry has used to share expertise among competing requirements and make better use of the Navy’s IDC. For example, a network analyst may not be needed for an entire work shift on a particular task, maybe four hours will suffice so the analyst could move on to another vital tasking. “This paradigm shift could lead to greater collaboration among the workforce and greater productivity,” Herbert said. “There can be no demarcation in IDC military jobs. The need to broaden job skills and enable resiliency across the IDC is imperative.”

Herbert said the Navy recently

conducted a three-week C5I (Command, Control, Communications, Computers, Combat Systems and Intelligence) review to better balance manning in the Navy’s IDC and to better align training requirements. The aim of training is beyond just the “buttonology” of learning a skill. Rather, the goal is for information systems technicians

“The Navy has much to offer cyberspace professionals ... and our IDC junior service members have far greater responsibilities than their counterparts and they value their contributions to national security.”

RDML Gretchen Herbert, Commander, NAVCYBERFOR

(ITs) and cryptologic technicians (CTs), for example, to be able to employ critical thinking skills and fundamental knowledge.

The Navy is evaluating individual skills training, education and systems training plans, as well as funding prioritization. For instance, the Navy’s new shipboard network, CANES — Consolidated Afloat Networks and Enterprise Services — is currently being installed on the USS Milius and within the next 10 years, CANES will be deployed to 192 ships in the Fleet. “ITs will have to be trained to defend and operate the new network,” Herbert said.

According to Herbert, the Navy is also looking at IDC officers’ mid-career and leadership training. But she suggested that the Navy should move away from service-specific parochial interests for greater sharing of training

resources with the other services.

“The Navy has much to offer cyberspace professionals,” Herbert said. In addition to the much coveted training Navy enlisted personnel receive in “A” schools and the opportunity to obtain commercial certifications, IDC junior service members have far greater responsibilities than their counterparts

in the commercial sector and the value they place on their contributions to national security remain significant recruiting and retention factors. “While perhaps the Navy cannot compete with commercial salaries, service members express job satisfaction with the challenging work they perform and identify strongly with the core values and culture of the Navy,” Herbert said.

Gill and Herbert said that the Marine Corps and the Navy are reviewing their Mission Essential Task Lists (METL) as another way to better align training to requirements. A METL is a list of tasks considered essential to the accomplishment of a mission and may include associated conditions, standards and supporting tasks. The Navy is also conducting training and education pilots. One example, which began in December 2012, is making graduate-

level education available to IDC officers and civilians through a new partnership with Carnegie Mellon University.

The panelists agreed that commercial IT certifications are important training tools and recruiting and retention incentives, and in some cases a Defense Department requirement to fill a position, but that more innovative ways of training are needed to ensure the cyberspace workforce keeps pace with technology advances and risks, especially in an era of fiscal austerity.

Each of the panelists praised the continued dedication to duty and extraordinary work of the DON’s cyberspace professionals in meeting increasingly greater demands to protect and defend the department’s cyberspace assets. The panelists said they want the members of the cyberspace workforce to know that their work is appreciated and their contributions to the DON are valued.

While there are no easy answers to the challenges, the panelists said the department is conducting multiple reviews to ensure that Navy and Marine Corps cyberspace training remains world-class and meets the needs of an unrivaled DON cyberspace workforce.

For more information about cybersecurity and the cyberspace workforce, please visit the DON CIO website: <http://www.doncio.navy.mil>.

EDITOR’S NOTE: Reprinted with permission from CHIPS magazine July -- September 2013 edition (Vol. XXXI, Issue III)



Young Patriots Share Ideas with not 1, but 2 Admirals

Story & Photos by Gary Nichols, CID Public Affairs



VADM Michael S. Rogers, commander of U.S. Fleet Cyber Command and U.S. 10th Fleet, chats with staff and students during lunch at the Gold Coast Café on board Corry Station.

PENSACOLA, FL – The commander of U.S. Fleet Cyber Command (FCC) and U.S. 10th Fleet visited staff and students at the Center for Information Dominance (CID) June 12.

This was the second visit to CID by VADM Michael S. Rogers since he assumed command of the Cyber Command and the 10th Fleet in September 2011.

“I’m delighted to host VADM Rogers again,” CID Commanding Officer CAPT

Susan Cerovsky said. “As our major stakeholder, it is absolutely critical we have these face-to-face meetings with the operational commander because they allow us to gain a better understanding of training and priorities now and in the future.”

FCC serves as the Navy Component Command to U.S. Strategic Command and U.S. Cyber Command, providing operational employment of the Navy’s cyber, network operations, information

operations, cryptologic/signals intelligence and space forces; and Navy’s Service Cryptologic Component commander to the National Security Agency/Central Security Service.

Tenth Fleet is the operational arm of FCC and executes its mission set through the same maritime warfighting organizations and mechanisms that the Navy uses in other warfighting domains.

Rogers said he is always thrilled to return to CID, where he began his career as a Navy cryptologist 26 years ago.

“It’s great to come back and remember things, comparing them to when I first got here,” Rogers said. “It’s also great to see how training continues to evolve as our challenges continue to change.”

The first step of that journey from a new accession Sailor to full-fledged cyber warrior begins at a CID schoolhouse.

CID is the Navy’s learning center that leads, manages and delivers Navy and joint forces training in information operations, information warfare, information technology, cryptology and intelligence.

“We have to be as operationally ready in the cyberspace area as we are in every other war fighting mission,” Rogers said. “Cyber readiness, like

readiness in all war fighting areas, is a team effort – it takes all of our teammates across the Navy.”

CID provides training for approximately 24,000 members of the U.S. Armed Services and allied forces each year. With a staff of nearly 1,300 military, civilian and contracted staff members, CID oversees the development and administration of 226 courses at four commands, two detachments, and 16 learning sites throughout the United States and Japan.

Joining Rogers for part of the day was RADM Don Quinn, commander, Naval Education and Training Command (NETC), which is located at nearby Naval Air Station Pensacola. Rogers and Quinn ate lunch with joint service students who were enrolled in the Joint Cyber Analysis Course (JCAC).

“It’s always great to see young men and women in the early stages of their journey in uniform,” Rogers said. “You know as someone who has been in the Navy now for 32 years, it’s interesting to look back and think about myself when I started that journey as a 21-year-old ensign; it’s great to see these young men and women who are willing to serve something bigger than themselves.”

... continued on Page 7



... continued from Page 6

One of those students Rogers chatted with during lunch was CTNS Maxime Dugas-Davis, of Blacksburg, VA.

She said when she joined the Navy, she never expected to dine with a three-star admiral.

"I'm grateful for the opportunity to be able to meet with someone like VADM Rogers, who has so much experience in the Navy, and to have had such an engaging conversation with him," Dugas-Davis said. "It was really awesome."

Quinn said the most satisfying part of his job is meeting bright young Sailors like Dugas-Davis, who are going through training at one of the many NETC Learning Centers, like CID.

"It's always a pleasure to meet with these outstanding young patriots who are at the beginning of their Navy career," said Quinn. "The skills of our people form the foundation of our Navy's combat readiness. Our training cultivates a culture that challenges the status quo and promotes unconventional solutions to complex problems. Quality training, like that provided at CID, is our Navy's asymmetric advantage in combat."

IT "A" school instructor CTR1(EXW)

Antonio L. Lucero, of Denver, said it was the highlight of his career to have lunch with the two flag officers.

"It is always a pleasure seeing the leaders of today's Navy getting engaged with the junior Sailors," Lucero said. "It was a great honor to have lunch with both VADM Rogers and RADM Quinn."

"The fact that in initial Navy training here we have Air Force, Army, Marines and Coast Guard, that they get exposed to a broader part of the team from the very beginning; I think that's a real positive," Rogers said.

"We must continue to develop an elite workforce that is recruited, trained and educated to better understand the cyber-environment, employ the latest technological advances, and deliver cyber war fighting capability anywhere

around the world."

"The bottom line is we continue to generate out of Pensacola trained, ready, motivated Sailors who want to get out, whether they are going to sea, whether they are going to one of our sites ashore around the world; this organization continues to produce motivated men and women who have the tools they need to roll up their sleeves and get out there and actually do it, and to keep learning," Rogers added. "We're very fortunate to have CID as a part of the Navy team. I feel energized every time I come down here." ✂



(Clockwise) VADM Rogers tours the command's display, a collection of historical cryptologic artifacts, on board Corry Station. Also pictured is retired CTCRM John Gustafson, who is a volunteer historian for the command display. VADM Rogers chats with staff and students during lunch at the Gold Coast Café on board Corry Station.



It's New, It's Effective . . . FOIAonline

The Department of the Navy will implement a new electronic Freedom of Information Act (FOIA) tool across the DON on Oct. 1, 2013.

FOIAonline is a cost-effective, multi-agency, shared service tool that meets all core FOIA requirements. It provides the public with a simplified web-enabled portal to request information from multiple agencies, track responses and access previously submitted requests and released records. The Environmental Protection Agency, Department of the Treasury, and National Archives and Records Administration launched FOIAonline earlier this year.

FOIAonline will provide the DON with the ability to:

- accept requests online and track requests in a case file;
- manage deadlines
- calculate fees
- research and upload records
- publish electronic records
- accept appeals online
- prepare the annual report
- search and retrieve FOIA requests and responsive documents.

Many DON organizations are currently using the Naval Sea Systems Command electronic FOIA tool. These organizations will continue to use the NAVSEA tool through the end of September 2013 and switch to the new tool when it is launched on Oct. 1.

For more information about the tool and its capabilities visit: <https://foiaonline.regulations.gov/foia/action/public/home>.

Cell Phone Signal Boosters May Not Boost

Recent changes in Federal Communications Commission (FCC) regulations governing signal

boosters enable the sale of certain types of these boosters within the United States. Signal boosters are devices that can improve cell phone coverage in areas where they do not get a good signal.

Navy and Marine Corps organizations considering these devices are reminded that FCC regulations only apply within the United States and its Possessions (US&P). Operations outside the US&P are regulated by host nation agreements that may not permit these signal boosters. Also, using signal boosters aboard naval ships, aircraft and installations requires special consideration for electromagnetic environmental

effects. Other requirements, such as the completion of a spectrum supportability risk assessment and registering technical parameters in the Equipment Location-Certification Information Database may also apply. The electromagnetic spectrum is a dynamic environment.

Before purchasing any radio frequency spectrum dependent device, Department of the Navy personnel are reminded to consult with local spectrum management or the Navy Marine Corps Spectrum Center at navyspectrum.fct@navy.mil.

How Many Lives Does Your SIPR Token Have?

90 Meter CIW (Certificate Issuance Workstation) Software

Did you know your SIPR Token certificates have a three (3) year life span? With this guide we will walk you through the process of how to check the expiration date of your token's certificates.

Please use the guide below to check and verify your certificates. If you have any questions, contact your command's Trusted Agent (TA) or Local Registration Authority (LRA).

1. Insert your token into the SIPR computer card reader and login.
2. Locate the 90 Meter Smart Card Manager icon.
 - a. WIN XP – located in task bar in lower right corner of screen
 - b. WIN 7 – located in the icon container box in the lower right corner of the screen
3. Right mouse click on the icon and

select "Show Interface".

4. On the interface click the "Certificate Browser" tab.
5. You should now see three certificates on the left side of the interface labeled Identity, Signing and Encipherment.
6. Left mouse click on one of the certificate icons.
7. Use the scroll bar and find the "Valid To" field. This is when your certificate will expire.
8. Repeat for the other two certificates. The dates should match as they were all created at the same time.
9. When finished close the interface by clicking the red "X" in the top right corner.

EDITOR'S NOTE: If your certificates are within 60 days of expiring you will need to contact the issuing TA / LRA.



DON CIO Awards Call for Nominations

The Department of the Navy Chief Information Officer is pleased to announce the call for nominations for the following FY 2013 awards:

About the Awards:

The DON IM/IT Excellence Awards recognize superior quality of IM/IT projects, teams, and individuals helping to transform the Navy and Marine Corps through information technology.

Named for the DON Principal Deputy Chief Information Officer who lost his courageous battle with cancer in June 2009, the Lussier Electromagnetic Spectrum Award is presented to an individual who demonstrates superior achievement in DON Electromagnetic Spectrum management and use.

The DON Cyberspace/IT Person of the Year and Rising Star of the Year Awards are two awards that were developed to acknowledge senior and junior level individuals who strive to deliver significant management efficiencies and cost savings to the department, through visionary thinking, innovation, and superior leadership skills.

Nomination Criteria:

Nomination criteria and information for each award are provided below. This same information is presented in a one-page table format for ease of use. Scroll down to the "Downloads" box below and click on the "DON CIO Awards Table" PDF to view and save the table.

Awards Submission:

To be considered for one of the DON CIO awards, please submit a nomination package at <http://go.usa>.

[gov/jTDB](http://go.usa) by Nov. 15, 2013. Award winners will be notified by email on or about Jan. 6, 2014. ✂

DON Virtualizes Servers Server Based Systems/Applications

On July 29, 2013, the Department of the Navy Chief Information Officer released the memo, "Server, System, and Application Virtualization," which stipulates that the DON must virtualize all current servers and server-based systems/applications. The process of virtualization will allow multiple operating systems and applications to be run on a single physical server, thus reducing operational costs and improving flexibility within the existing information technology infrastructure. Virtualization is one of the multiple efficiency efforts that the DON must pursue to achieve cost reductions.

Plans for virtualization are requested from DON Deputy CIO (Navy), DON Deputy CIO (Marine Corps), and DON Assistant for Administration (DON/AA) within 120 days of release of this memo. Plans must include the following:

- Conversion of a minimum of 15 percent of each Budget Submitting Office's computing environment per year until 100 percent virtualization is achieved. Conversion of a minimum of 15 percent of each Budget Submitting Office's computing environment per year until 100 percent virtualization is achieved.
- Enterprise virtualization platform standards established by the Navy and Marine Corps Technical Authorities.
- Compliance with published Technical Authority standards.
- A process to provide quarterly progress reports

to the DON CIO.

- A process to ensure that all future systems and applications are developed to deploy and operate in a virtualized environment.
- A process to ensure that all future systems and applications are developed to deploy and operate in a virtualized environment.

All new servers and server-based systems/applications not already approved for deployment as of the date of this memo must be developed to operate in virtualized environments.

Owners of systems/applications who deem their systems/applications incapable of virtualization must submit waiver requests endorsed by DON Deputy CIO (Navy), DON Deputy CIO (Marine Corps), or DON/AA for DON CIO approval by Sept. 30, 2014. No permanent waivers will be granted; waivers will be good for one year and reconsidered during subsequent annual reviews. ✂





Vulnerability Scans Required for Navy Website Health

By Diana Boudreau, NWRAC Technical Lead

The Navy's Web Risk Assessment Cell (NWRAC) is part of Navy Information Operations Command (NIOC) Norfolk and tasked with conducting compliance scans of navy public accessible websites. However, conducting compliance-only scans does not fully address the real-world threat posed by adversaries aggregating data from websites or injecting malicious code. To mitigate these types of vulnerabilities, the NWRAC will conduct compliancy, content and technical vulnerability scans of all unclassified Navy public accessible websites designed, developed, procured or managed by Navy activities or by contractors on behalf of those activities.

The appearance, accuracy, currency and relevance of the information presented by Navy commands on their websites reflects on the Department of the Navy's (DON) professional standards and credibility. Additionally, information residing on a web server associated with a "navy.mil" domain is interpreted by the worldwide public, US citizens and media as reflecting official Navy policies or positions. Therefore, all information presented must be accurate, current, and in line with DON policies. The same is true for Navy websites allowed to publish outside of the "navy.mil" domain, for example, www.university.edu/nrotc.

The ultimate responsibility for protecting websites, posting

content, and meeting administrative compliance standards resides with each commanding officer. While this and the guidelines for technically securing websites and securing privacy information have been widely known, there continues to be widespread issues that put Navy personnel, operations and information at risk.

As the Navy's central operational authority for networks, part of US Fleet Cyber Command's (FCC) mission is to ensure operational integrity and security of the computers and networks supporting navy websites. In doing

"The ultimate responsibility for protecting websites, posting content, and meeting administrative compliance standards resides with commanding officers."

so, FCC/ Commander, Tenth Fleet (C10F) tasked NIOC Norfolk NWRAC with conducting

vulnerability scans against official Navy public websites to detect the most common web application vulnerabilities.

The NWRAC will conduct technical vulnerability assessments and compliancy scans of unclassified Navy public accessible websites at least tri-annually to identify potential vulnerabilities resident on Navy websites and ensure websites meet compliancy standards established in SECNAVINST 5720.44C. Vulnerability assessments include scanning against a command's website (not hardware platform) using commercially available web application scanning software and

... continued on Page 13

Graphic Illustration by MC2(SW) Jacob Galito, NAVCYBERFOR Public Affairs



Try Keeping Up With This Jones . . .

Former IT3 shares his love for Navy with others through Mentorship

By MC1(IDW/SW/AW) Elizabeth Burke, NETWARCOM Staff Journalist

When LTJG Patrick Jones enlisted in the Navy in November 2003, he attended Information Systems Technician (IT) "A" school and was assigned to the aircraft carrier USS Harry S. Truman (CVN 75).

While on a six month deployment his chief urged him to attend a Naval Academy informational meeting held by the Command Career Counselor. He reluctantly went to the brief believing he did not have a chance at being accepted. The presentation kindled an interest that began the application process in October 2004.

Just a few years earlier his life lacked focus. In 2001, his junior year of high school, his family moved away from his childhood home and he began attending a new high school. When the year concluded Jones made the decision to move in with his Grandmother in Sykesville, MD, to attend his old school and graduate with his friends. He was good at math and science but beginning his senior year in 2001 he still hadn't taken the SATs. He met with a guidance counselor who helped him sign up to take the SATs. Jones applied for admission to Virginia Tech and was accepted.

He went to college because that is what he thought he was supposed to do, but it was during his first year at Virginia Tech that the magnitude of being the first in his family to go to college, his perceptions of his family's expectations of him and the guilt of the financial burden this was putting on his family all became too difficult for him to handle. Telling his Grandmother that he would not be returning to Virginia Tech was the hardest thing he had to do, "because she was the one person I didn't want to disappoint," Jones said.

He returned to Sykesville and worked locally. During a discussion with his uncle about his future they disagreed on his direction in life. Out of spite he went

to the Navy recruiter and enlisted.

Back aboard the Harry S. Truman (CVN 75), in November of 2004 he was advanced to Petty Officer 3rd class and in February 2005, IT3 Jones earned his Enlisted Surface Warfare Specialist (ESWS) and Enlisted Aviation Warfare Specialist (EAWS) qualifications. IT3 Jones began to believe that his recent advancement and ESWS and EAWS qualifications would make him more competitive as a Naval Academy candidate. That same month he was offered an appointment to the Naval Academy class of 2010, upon the completion of the Naval Academy Preparatory School (NAPS). The mission of the Naval Academy Preparatory School is to enhance midshipman candidates' moral, mental, and physical foundations to prepare them for success at the U.S. Naval Academy. While at NAPS Jones also advanced to IT2.

Jones entered the Naval Academy in June 2006 and studied Electrical Engineering. He was commissioned in 2010 and elected to pursue an aviation career. He attended flight school in Pensacola, FL and Vance AFB, OK. One third of the way into his flight training at Vance AFB, he began to question if being a pilot was the career track he really wanted to pursue. He was released from training and entered a pool of officers awaiting reassignment.

While awaiting reassignment Jones received a phone call from the Information Professional (IP) Community Manager. The Information Professional career field is relatively new compared to other warfare areas. He was offered the opportunity to enter the IP career field and after a brief training period



ADM Bill Gortney, commander of U.S. Fleet Forces, shakes hands with LTJG Jones after presenting him with his IDWO pin. (Photo by Robin Hicks)

reported to Naval Network Warfare Command as a Battle Watch Captain, in training, in 2012.

Jones did not have a linear career path. What he enjoys most about the Navy is the opportunity he has to lead, mentor and develop junior Sailors who may not have had the most direct path in their Navy career. He is currently mentoring one Sailor who is applying to the Naval Academy and one who has already been appointed to the class of 2017.

"Developing a relationship with others and assisting them accomplish their unique goals and ambitions offers me more satisfaction than any personal qualification or award ever, ever will," said Jones.

His next assignment is the USS Kearsarge (LHD 3), as the Cyber Security Officer and Information Assurance Manager.

"As long as the Navy continues to afford me opportunities and challenges not only myself but others to grow and develop," said Jones. "I will continue to serve." ✂



Cyber Cat's Tips

Protecting & Avoiding Becoming Victim of Ransomware

Articles by Laurie Cummings, CISSP CYBERFOR IAM

Scammers are using a form of malware called Ransomware to terrorize computer users. This type of malware prevents a user from using his or her computer or accessing any data until a payment (the ransom) is made. The user is asked to pay a ransom -- that ranges anywhere from hundreds to thousands of dollars -- through wire transfer, online payment vouchers or premium rate text messages. Users could feel forced to pay in order to

have access to their system again.

The system is held hostage in several ways. Lockscreen Ransomware displays a full-screen image or webpage that prevents access to anything on your computer. Whereas, encryption based Ransomware encrypts the files with a password, and this takes away your ability to open or copy files.

Some instances of Ransomware display a notification, saying the local authorities have detected

illegal activity in your computer.

Some users are told their computers contain pornography, illegally obtained software, illegally downloaded music or something else linked to illegal activity. Other users are told the version of their operating system is counterfeit and they must purchase a good, clean copy before their computer can be used again.

This virus is presenting so many problems because it appears to come

from actual law enforcement officials with very real looking web pages and official seals and logos. This scam is not only directed at the home user with one or two computers, but also at large corporations and hospitals that can afford to pay higher ransoms.

How do criminals install Ransomware on your computer? Ransomware is usually installed

... continued on Page 13



... CAT TIPS from Page 12

when you open a malicious email attachment or when you click a malicious link in an email message, instant message, or on a social networking site.

The Microsoft Safety & Security Center recommends several ways to avoid becoming a victim of Ransomware:

- Keep all of the software on your computer up to date.
- Keep your firewall turned on.
- Don't open spam email messages or click links on suspicious websites.
- Download Microsoft Security Essentials, or Anti-Virus software
- Scan your computer with the Microsoft Safety Scanner, or Anti-Virus software

Under no circumstance should you pay the ransom in order to regain access to your computer or files. If you pay, that does not guarantee you will be given access to your files. The scammers could continue to ask for more money. What you should do is immediately report the incident to: <http://www.onguardonline.gov/>.

If you find out your computer has Ransomware on it, you should immediately take steps to remove it. This link will help you remove it: <http://www.microsoft.com/security/portal/shared/>

[ransomware.aspx#recover](#).

Remember, never visit questionable websites or download suspicious attachments. Make sure you only open emails from people you know and be vigilant when doing online transactions. ✂

Use Common Sense or Get Phished

A new spear phishing campaign directed against the government targeting U.S. personnel affecting theme for one or more anti-virus programs.

Please use caution as these socially-engineered attacks continue, it is important to remember safe email practices. Users should be wary of opening attachments or clicking links contained in emails from senders with whom the recipient is not familiar, even if they appear legitimate at first glance.

If unsure of the legitimacy of an attachment or link, contact the sender of the email to verify that this was in fact sent by that person. Attachments can contain malware that may not be detectable to the average computer user. If the attachment looks suspicious, do not open it. If moving the mouse over a link gives the user a different URL than what appears in the email, or if the link looks unofficial, it may be malicious. ✂

EDITOR'S NOTE: *Article taken from "On Cyber Patrol" & adapted to fit the Navy environment.*

... WEBSITE HEALTH from Page 10

are conducted remotely from NIOC Norfolk. All assessments are overt, cooperative and well coordinated with the assessed command, web hosting facility, Navy Cyber Defense Operations Command (NCDOC) and NIOC Norfolk. Compliancy scans are Administrative in nature (e.g., DOD warning banners, required links).

Another component of the assessment is to conduct Operations Security (OPSEC) content reviews for classified, Critical Information (CI) and Controlled Unclassified Information (CUI) to include Personally Identifiable Information (PII) resident on unclassified Navy websites.

The NWRAC will notify the responsible command and echelon II level commander when a website is discovered to be at risk for technical vulnerability, exploitation, OPSEC content or compliancy concerns. Also, they will provide findings and recommended corrective actions in a comprehensive report issued to the website content owner, NCDOC, web hosting facility, FCC/ C10F and content owners Immediate Superior in Charge (ISIC).

All Navy commands and activities that maintain an official Navy public accessible website must implement and administer a comprehensive unclassified website management program to include:

- Registering their website with NIOC Norfolk at <http://www.public.navy.mil/fcc-c10f/niocnorfolk/pages/registeryoursite.aspx>. Persons

responsible for each website will review and re-register their website on an annual basis or whenever there is a change in any of the required registration data fields, for example the webmaster or Public Affairs Officer.

- Register their website with DON Application Database Management System (DADMS) at <https://www.dadms.navy.mil/>. Registering with NIOC Norfolk does not meet the requirement for commands or activities to register with DADMS.
- Completing the self-assessment checklist annually. The checklist is available at <http://www.public.navy.mil/fcc-C10f/niocnorfolk/pages/registeryoursite.aspx>.
- Developing local procedures to ensure the approval of information prior to posting on command or activity websites. At a minimum, this process shall include review by the PAO in coordination with the OPSEC officer, information assurance personnel and the webmaster. Information not suitable for worldwide release may only be placed on a Department of Defense (DOD) Public Key Infrastructure (PKI) protected site. Domain restriction alone is not sufficient.

For more information on requirements for Official Navy Public Accessible websites, to schedule a technical vulnerability assessment or inquiries on other services the NWRAC provide, email wra_reporting@niocnorfolk.navy.mil or call (757) 417-4158x0. ✂





CID CO Visits Pensacola's 'Panhandle' Tiger Bay Club

Story & Photos by Gary Nichols, Center for Information Dominance Public Affairs

PENSACOLA, FL – CAPT Susan K. Cerovsky, commanding officer of the Center for Information Dominance (CID), recently spoke to members of the Pensacola Tiger Bay Club at the New World Landing in downtown Pensacola.

Vice President of Program, Jolinda Jones, said she had heard Cerovsky speak last fall at the Pensacola Rotary Club and requested that Cerovsky speak to her group.

The Panhandle Tiger Bay Club, established in 1977 by the late Pensacola News Journal columnist Pat Lloyd and John Broxson, is a diverse, non-partisan group of men and women who are interested in public policy issues and politics. The club brings in speakers who address topical issues and present ideas that are intended to provoke curiosity and provide insight, as well as generate debate and community discussion.

The Panhandle Tiger Bay Club holds monthly luncheon programs and an annual dinner meeting. Past speakers have included Martha Raddatz and Claire Shipman of ABC News, political commentator and columnist Dick Morris, Jeff Birnbaum of the Washington Post, and pollster John Zogby.

Although she was speaking to a diverse group, there was one thing they all shared in common: they all had personal smart devices, and were all connected to the internet.

Cerovsky asked for a show of hands of anyone in the audience that had a cell phone, smart phone, tablet, e-reader or computer.



CAPT Susan K. Cerovsky responds to a question-and-answer session following her address to club members.

She wasn't too surprised when every hand in the room shot up.

This emphasized the point to the audience of how many people – not just in that room, but across our society and the globe – have become integrated into and dependent on the internet for much more than just e-mail and paying bills.

"For many of us, the thought of being unplugged is almost unthinkable," Cerovsky said.

For many in the audience, CID is a non-descript

base on the west end of Pensacola, and they were a bit fuzzy on its training mission and how CID impacts national security.

She explained that CID is the Navy's learning center that leads, manages and delivers Navy and joint force training in information operations, information warfare, information technology, cryptology and intelligence.

There was also a mistaken notion that CID exists only in Pensacola.

Cerovsky explained that CID's footprint is vast, with schoolhouses ranging from New England to the West Coast, Hawaii and Japan, and personnel from all the armed services learn to defend and maintain those vital networks everyone in the room has come to depend on.

Cerovsky then discussed current threats, such as phishing, spear phishing, whaling, tab nabbing and others the members might encounter on their own computers.

At the end of the discussion, Cerovsky left the members with one final bit of advice regarding unknown links or e-mails.

"Remember," she said. "When in doubt, DELETE; Do NOT open unknown files; Do NOT click on unknown URLs; Do NOT open images or audio files. Again, when in doubt, DELETE."

Jones explained that club members, if they had questions for Cerovsky, could fill out a query card that was available on each table and submit it for a

[... continued on Page 15](#)



... continued from Page 14

question-and-answer session at the end of her talk.

“We had a number of questions submitted, but ran out of time before we could ask CAPT Cerovsky to respond to all of them,” Jones said.

At the end of Cerovsky’s 40-minute talk, she fielded questions from the podium for another half hour. Clearly interested in what she had to say, many club members stayed behind while the room was being cleaned to chat with Cerovsky for another 20-30 minutes.

“How gracious of her to spend so much time afterward answering questions and meeting our members! They were clearly delighted by her,” Jones said. “We rarely have people staying for so long after a meeting, but Capt. Cerovsky went out of her way to listen and interact with each person wanting to talk with her.”

With a staff of nearly 1,300 military, civilian and contracted staff members, CID oversees the development and administration of 226 courses at four commands, two detachments, and 16 learning sites throughout the United States and Japan. CID provides training for approximately 24,000 members of the U.S. Armed Services and allied forces each year. ✘



Pensacola Tiger Bay Club members listen intently to a talk by CAPT Susan K. Cerovsky at the New World Landing in downtown Pensacola. She discussed the training mission of CID and the role it plays in defending national security.

San Diego Sailors Celebrate Space Day on Earth

By CID Public Affairs

SAN DIEGO – Sailors assigned to Center for Information Dominance Learning Site (CID LS) San Diego recently visited the San Diego Air and Space Museum to participate in the 10th annual Space Day celebration.

“This was a great opportunity for the Navy’s Information Dominance Corps (IDC) to represent themselves to the local community,” LTJG James Whitman, director for CID LS San Diego, said. “Just the day before this event, one of the Sailors was pinned with their Enlisted Information Dominance Warfare Specialists device; it’s outstanding to see these Sailors giving

back and sharing their knowledge of the IDC to the community.”

CID LS San Diego’s mission is to deliver full spectrum Cyber Information Warfare, and Intelligence Training to achieve decision superiority. In addition to their military duties,

CID LS San Diego provides mentors,

tutors and role models for various organizations throughout San Diego County.

“The children were really interested in the Navy’s role in recovering future space

capsules,” CTR1 James R. Lee said, “This is our second event with the Air & Space Museum; last month we assisted in their annual Paper Airplane festival.”

Additionally, Lee operated the museum’s radio controlled blimp while explaining the role of Unmanned Aerial Vehicles to the Navy’s mission.

The Sailors had the pleasure of meeting Astronaut Garrett Reisman. Reisman has flown on Space Shuttles Endeavour, Discovery and Atlantis during his astronaut career, and completed three successful space walks.



Sailors from CID Learning Site, San Diego pause for a photo during their second event with San Diego’s Air and Space Museum. (U.S. Navy Photo)

... continued on Page 16



. . . continued from Page 15

Sailors who participated in the event said they enjoyed the opportunity to interact with the guests and represent the Navy.

The San Diego Air & Space Museum

was established Oct. 12, 1961, to preserve, inspire, educate and celebrate Air & Space history.

In 1986 the Museum became the first aero-themed museum

to be accredited by the American Association of Museums, and it is now a Smithsonian affiliate. The California Legislature voted to declare the Museum "California's official Air and

Space Museum and Education Center." The Museum is recognized as one of the country's premier aerospace museums. ✂

“Motivatation Pays Off”

Norfolk Sailor Chosen for National Intelligence University

By ITC Ariel Anderson, CID Public Affairs

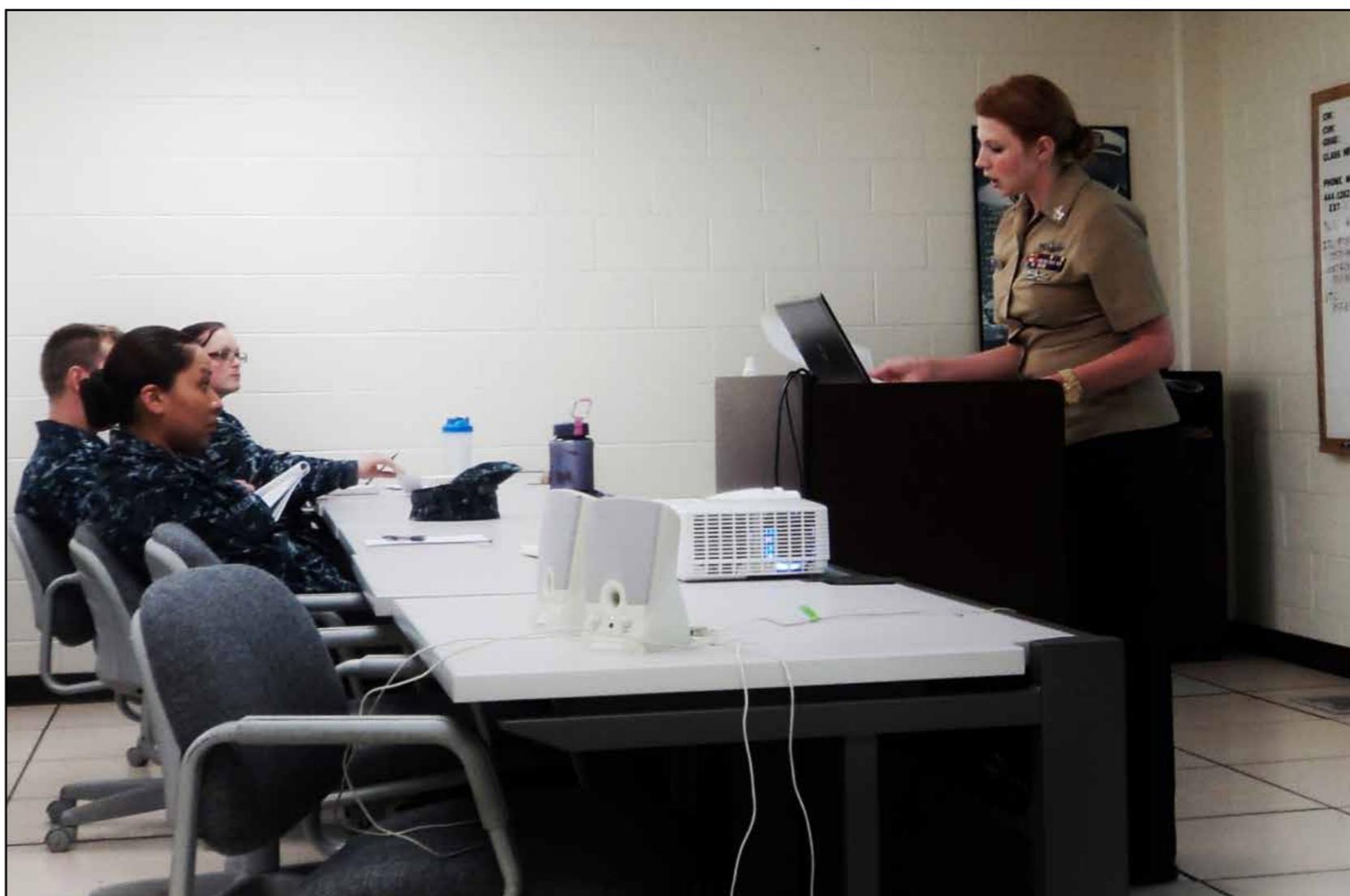
VIRGINIA BEACH, VA – A Center for Information Dominance (CID) Learning Site (LS) Norfolk Sailor is preparing for her latest personal challenge, after her selection to attend the National Intelligence University (NIU) starting in August 2013. Upon graduation she will be commissioned an Information Warfare Officer.

IT1(IDW/SW/AW) Amanda Montgomery of CID LS Norfolk's Information Systems department said her acceptance into a commissioning program marks the fulfillment of one of her most important career goals; a goal she has worked hard to achieve since she enlisted in the Navy almost eight years ago.

“I applied for the Seaman to Admiral program in 2006 and 2007, and even though I was not selected I stayed motivated and did not let that deter my goals to further my career,” said Montgomery.

While stationed on USS Wasp (LHD 1), Montgomery decided to enhance her Navy career and get a head start on her educational goals. In the four years on board Wasp, she completed all of her general educational requirements for a bachelor's degree in cyber security through Navy College Program for Afloat College Education (NCPACE) and University of Maryland University College.

. . . continued on Page 17



(Right) IT1(IDW/SW/AW) Amanda Montgomery instructs CID Learning Site Norfolk students on the finer points of Information Systems training. (Photo by MCSN Jackie Hart)



... continued from Page 16

Montgomery currently serves as an instructor delivering systems administration training to students in the information technology field. It is there that she applied for the Direct Commissioning Program (DC) at NIU.

“In 2011 I was introduced to the National Intelligence University DC officer by my Chief. I started my application a year prior to the deadline, which consisted of a personal statement, nomination from the command, 80 hours towards my bachelor’s degree, and my evaluations as a Sailor,” said Montgomery. “This program seemed like the light at the end of the tunnel as far as my career goals because it paired my experience in cyber security field with my ultimate goal of working with intelligence and cyber terrorism.”

Montgomery’s relentless dedication to her commissioning goals has had immense influence within her department as well as her division. Sailors under Montgomery’s supervision said they enjoy working with such a dynamic and motivating leader.

“Working with Petty Officer Montgomery has been both a rewarding and profound experience that has set the standard for what I expect of

myself in my career. She continuously demonstrates a level of knowledge and professionalism, coupled with a genuine devotion to making the workplace a more satisfying and gratifying experience that is the model for everyone who has the pleasure of working with her,” IT2(SS) Timothy Whiteside said. “I hope that every command has at least one Sailor that demonstrates the level of honor, courage and

commitment that Petty Officer Montgomery brings to work every day.”

Montgomery explained she always advises her Sailors and students to stay driven and enthused in reaching their career goals as well as performing their duties. Her supervisors as well praise the way she operates at CID LS Norfolk.

“Petty Officer Montgomery has always been one of the top performers at the command,” ITC(IDW/EXW/SW) Rick Colonno said. “She excels at everything she does so it was no surprise to me that she was selected for this program.”

For Montgomery, her selection to NIU marks the beginning of a new chapter in her Navy career and she’s confident her enlisted experience will help her in the commissioned ranks.

“I have already served time as an enlisted Sailor, so I think I’ll have the respect I need to lead a prosperous division of Sailors wherever I’m stationed,” Montgomery said. “I’ll be a better listener and a more pronounced leader because I’ve already been in their place, and I won’t forget where I started.”

CID is the Navy’s Learning Center that leads, manages and delivers Navy and Joint Force training in information operations, information warfare, information technology, cryptology and intelligence. ✂



CID Learning Site Norfolk Instructor IT1(IDW/SW/AW) Amanda Montgomery (right) with CID Learning Site Norfolk, Senior Enlisted Leader ITCM(IDW/SW) Sarah Gomez at Walker Hall on board Dam Neck Annex following a frocking ceremony. Montgomery was selected to attend the National Intelligence University (NIU) starting in August 2013. Upon graduation she will ultimately receive a commission as an Information Warfare Officer. (Photo by MCSN Jackie Hart)



TRAINING FOR NOTHING

AND THE SMEs FOR FREE ... FOR NOW





Hugh Chin, Fleet Logistics Center Norfolk, (left) and Johnny Fuller, Engility Corp, (right) where two subject matter experts at the Fleet Applications and Solution Team (FAST) training held at the Afloat Training Group Auditorium, Naval Station Norfolk. (Photo by Jacky Fisher)

By Jacky Fisher, NAVCYBERFOR Public Affairs

Who says you can't get something for nothing these days? With zero dollars spent on the second iteration of a FAST – Fleet Applications and Solutions Team – workshop, the Fleet Functional Area Manager (FAM) department of Navy Cyber Forces (NAVCYBERFOR) sponsored another successful workshop for more than 170 waterfront Sailors on the proper usage of several Fleet-wide afloat applications. The training workshop was held at the Afloat Training Group Auditorium, Naval Station Norfolk, and was open to all waterfront commands.

Specific applications selected for the Norfolk workshop were identified from survey results of more than 1,000

Operating System Environment (COMPOSE) Application Discovery Tool; Navy Cash; Navy Standard Integrated Personnel System (NSIPS); Planned Maintenance System Scheduler (PMS Sked) Version 3.2; Naval Tactical Command Support System (NTCSS); Shipboard Non-Tactical Automated Data Processing Program (SNAP); Automated Medical System (SAMsv8); Theater Medical Information Program (TMIP) SAMsv9; Enterprise Shift Operation Management System (ESOMS); and Food Service Management (FSM). MONEY TALKS...or at least got the ball rolling.

During a visit to USS Oak Hill in 2010, ADM John Harvey, then commander, U.S. Fleet Forces Command

Sailors. Targeted apps, used on both ships and submarines, ran the necessary gamut from quality of life to mission critical. Norfolk's training focused on the following apps:

Common Personal Computer (PC)

(FLTFORCOM), got an earful from a disgruntled Sailor experiencing difficulty accessing his bank account through the shipboard application, Navy Cash, designed to allow Sailors access to their money in a cashless environment. Navy Cash is on board 147 ships and processes approximately \$32 million a month.

With a closer look into the issue, NAVCYBERFOR discovered that many other applications and systems needed to be 'fixed', with issues spanning from apps functionality problems, security and interoperability issues and underfunded programmatic support – including training.

FLTFORCOM tasked NAVCYBERFOR to solve the problem. Fleet FAM led the charge by conducting a survey with Type Commanders (TYCOMs) and afloat commands

to identify all applications in the Fleet and which of them were failing the Sailor.

The mission was quickly identified - decrease security vulnerabilities, remove bandwidth hogs (old or redundant applications), and work with

Program Offices to identify required fixes and expedite them to the Fleet. A survey is a survey is a survey...not so FAST.

FAST uses a survey system with a 360-degree criterion in mind. Through shipboard visits, Sailors interact face-to-face with FAST team members to discuss issues, receive assistance, evaluate network scans and provide feedback to NAVCYBERFOR and the platform TYCOMs. During these visits, the FAST operates a survey system where Sailors are asked to outline issues they experience with shipboard apps. FAM and FAST then coordinated with the Program Offices that owned the troubled application or system to determine a solution. Based on these survey responses, FAST selected the top ten 'problem' apps and worked with the



Bruce Burkett (right) and Brian Holbert from Navy Cyber Forces discuss shipboard computer applications and the Fleet Applications and Solutions Team (FAST) Survey with LTJG Nicholas Hart, Navigator. (Photo by Robin Hicks)





Ken Brown, (center) a member of Navy Cyber Forces' FAST team discusses shipboard computer applications with IT2 Rocky Fuqua. (Photo by Robin Hicks)

Program Offices to tailor training based on Sailors concerns.

"Today's technical environment dictates the use of apps to get the job done. The funding isn't there to send every Sailor to formal training, so by default, Sailors themselves become the SMEs," said CDR Rich Menard, NAVCYBERFOR Fleet FAM. "FAST training is essential for Sailors to better understand how to fully use these apps. There's no better way to determine the needs of the deckplate Sailor except to speak directly to them."

NAVCYBERFOR sponsors and coordinates these workshops, but the SMEs come from the Program Offices supporting individual applications. Fortunately, the Program Offices have representative SMEs on both coasts, which allowed NAVCYBERFOR to host

the west coast workshop this past February in San Diego and the Norfolk workshop in June.

For now, although much coordination was needed to get these workshops off the ground, the training line of accounting has been kept to zero. But the need to have FAST take

their show on the road and hit multiple Fleet concentration areas worldwide is apparent and that is where an issue could come up given the current DoD-wide fiscal climate.

"RDML (Gretchen) Herbert (commander, Navy Cyber Forces) is 100 percent behind FAST's mission," said Menard. "We want to make contact with as many operational 'end users' as possible. It's not just about training Sailors on existing apps; FAST wants to also ensure training is in place for future apps introduced to the Fleet."

The training environment isn't all that unique - a briefer, a PowerPoint presentation and an audience. But it is distinctive in one essential way. Sailors from various waterfront commands with different issues, individual work situations, computer work stations,

versions and updates, can ask questions directly to the SMEs. Oftentimes Sailors from other commands had similar issues or were prompted to ask questions specific to their situation. Everyone benefited in this 360 degree training environment. Sailors speak directly to SMEs and are given real-time, current responses to their issue.

The first training held in San Diego last February was a success. Attendance increased with the Norfolk site and the feedback forms read pretty much the same - Sailors from both coasts praised the training.

From one Sailors critique sheet, "More Fleet involvement! More commands should have attended; maybe (make it) mandatory." And to complement the training environment, both East and West coast Sailors requested the use of laptops to make it

more interactive.

With successful training now bumping up against a constrained fiscal environment, it's difficult to predict what will happen in the future. "If the Navy provides the funding to continue FAST training in other Fleet concentration areas," said Menard, "we're ready to answer the call."

An afloat command can request a FAST visit by contacting the NAVCYBERFOR Fleet FAM department at richard.menard@navy.mil or john.toomer@navy.mil. Additional application support and/or training can be requested by contacting Navy 311. ✕

Editors Note: See the Spring & Summer 2012 edition of InfoDOMAIN, "One Way To Make Sailors' Lives Easier? Fix Their Software!" story for background information about how FAST came in to existence.

**Got a question and training is not scheduled in your area?
Help is still available.**

Navy 311 provides 24/7/365 customer support to the Fleet:

Phone: 1-855-NAVY311 (1-855-628-9311)

DSN: 510-NAVY311 (510-628-9311)

Email: Navy311@navy.mil (unclassified)

Navy311@navy.smil.mil (classified)

Navy message: NAVY THREE ONE ONE NORFOLK VA

Web: www.Navy311.navy.mil (unclassified)

www.Navy311.navy.smil.mil (classified)

Text: type Navy311@navy.mil into the TO line of text message

Navy311 Chat is available via website or mobile phone.

Sailor 2.1, a SPAWAR CAC-enabled self-help website is accessible at:

<https://sailor.nmci.navy.mil/Authentication/LoginForm.cfm>



Second Satellite to Boost DoD Satellite Communications

By Steven A. Davis, Space and Naval Warfare Systems Command Public Affairs

CAPE CANAVERAL AIR FORCE STATION,

FL -- The Navy's second Mobile User Objective System satellite was launched July 19 at 9:00 a.m. EST from Space Launch Complex 41. The successful launch represents a key step in providing enhanced satellite communications for the Navy and Department of Defense (DoD).

MUOS is a next-generation narrowband tactical satellite communications system designed to significantly improve beyond-line-of-sight communications for U.S. forces on the move. MUOS will provide military users 10 times more communications capacity over the existing system by leveraging 3G mobile technology, including simultaneous voice and data capability.

"The MUOS-2 launch is an especially significant event for the program because not only are we launching the second satellite, but the ground system, the networking software and the waveform are all aligning at the same time," explained CDR Matt Bohlin, the MUOS principal assistant program manager. "With MUOS-2 on-orbit this fall, we'll be testing the full system with all the new capabilities that it brings to the warfighter."

The first MUOS satellite, launched in February 2012 and accepted for operational use by U.S. Strategic Command in November, has been providing high quality voice communications for users.

The Navy plays a key role in national space efforts by providing narrowband satellite communications for the DoD and other government agencies. MUOS satellite communications capability is designed for mobile users who require high-speed mission data with higher data rates and improved operational availability.

Bohlin says users requiring these essential services will soon see significantly improved benefits when the full system suite comes on-line.

"Users are going to notice more bandwidth . . . and better connectivity. It will be a revolutionary leap for satellite communications for DoD."

CDR Matt Bohlin

weather." he said. "It will be a revolutionary leap for satellite communications for DoD."

With current capability, tactical users have limited access to narrowband satellite communications, and channels must be preplanned and allocated. Additionally, dismounted users had to be stationary to acquire the satellite.

With MUOS, users will have access on demand and be able to use the service while on the move and in all environments and weather to talk to beyond-line-of-sight recipients, whether they are on the other

. . . continued on Page 22



The Navy's Mobile User Objective System (MUOS) 2 satellite is encapsulated inside a 5-meter diameter payload fairing before being mated with an Atlas V rocket. MUOS is a next-generation narrow band tactical satellite communications system designed to significantly improve beyond-line-of-sight communications for U.S. forces on the move.

(Photo by Carl Winebarger)



... continued from Page 21

side of a mountain or the other side of the world.

Services will also be available for platforms such as ships, aircraft and vehicles.

Over the next several days, the satellite, which functions much like a cell tower in space, will transition to its geosynchronous orbit location 22,000 miles above the earth. Its solar arrays and mesh antennas will then be deployed and on-orbit testing will begin for eventual commissioning

into service.

The constellation of four satellites and one on-orbit spare will extend narrowband communications availability well past 2025.

The Space and Naval Warfare Systems Command, San Diego, the Navy's Program Executive Office for Space Systems, Chantilly, Va., and its Communications Satellite Program Office, San Diego, are responsible for the MUOS program.

Additional imagery, videos and launch coverage can be found at the Space and Naval Warfare Systems Command website link here [www.
public.navy.mil/spawar/Press/Pages/
MUOS-2.aspx](http://www.public.navy.mil/spawar/Press/Pages/MUOS-2.aspx).



(Left) A payload fairing containing the Navy's Mobile User Objective System (MUOS) 2 satellite is mated to an Atlas V rocket in the Vertical Integration Facility at Space Launch Complex-41 at Cape Canaveral Air Force Station, FL. MUOS is a next-generation narrow band tactical satellite communications system designed to significantly improve beyond-line-of-sight communications for U.S. forces on the move. (Photo by Gina Mitchell-Ryall)

(Right) An Atlas V rocket launches the Navy's Mobile User Objective System (MUOS) 2 satellite from Space Launch Complex-41 at Cape Canaveral Air Force Station, FL. MUOS is a next-generation narrow band tactical satellite communications system designed to significantly improve beyond-line-of-sight communications for U.S. forces on the move. (Photo by Patrick H. Corkery)



RESCUE AIRMEN SUPPORT HISTORIC ROCKET LAUNCH

Story & Photos by Tech. Sgt. Anna-Marie Wyant, 920th Rescue Wing Public Affairs

PATRICK AIR FORCE BASE, FL -- Reserve Airmen from the 920th Rescue Wing supported the successful launch of an Atlas V rocket July 19 at 9 a.m. EDT from Space Complex 41, Cape Canaveral Air Force Station.

Rescue Wing Airmen took flight on two HH-60G Pave Hawk helicopters more than two hours before the scheduled launches. They patrolled the stretch of the Atlantic Ocean beneath the launch trajectory ensuring no mariners veered into harm's way of potential rocket debris hazards, maintaining the security and safety of the range.

"With all the boats out in the ocean moving around in various directions, first we have to find out where they are, where they're going, and where they will be at the time of the launch," said Lt. Col. Robert Haston, a 920th Rescue Wing Pave Hawk pilot who flew on this mission. "So we prevent boats from being within the range at launch time."

This launch marked the largest ever payload for an Atlas V rocket. Haston said due to both the size of the load and the size of the rocket itself, the range clearing area covered an area expanding approximately 60 miles from the launch site.

Range clearing is one of the many tasks that the Airmen of the 920th RQW are charged with. The premier combat-search-and-rescue wing Airmen are

trained to provide search and rescue services in humanitarian and combat environments.

According to the United Launch Alliance, the rocket launched with the Mobile User Objective System-2 satellite, which will ensure continued mission capability of the existing ultra-high frequency satellite communications system, and represents deployment of the second satellite in the next-generation narrowband tactical satellite communications system that will provide significantly improved and assured communications for the mobile military members.

The MUOS will ultimately provide military users with 10 times more communications capacity over existing systems, including simultaneous voice and data, leveraging 3G mobile communications technology. The MUOS-2 satellite will cover approximately a third of the Earth's surface. ✂



(Clockwise) Lt. Col. Robert Haston and Capt. Jason Tomas, 920th Rescue Wing Pave Hawk helicopter pilots at Patrick Air Force Base, Fla., prepare to fly over Florida's Atlantic Coast to provide range clearing support for the Atlas V rocket launch July 19, 2013, Cape Canaveral Air Force Station, FL.

An Atlas V rocket takes off July 19, 2013 from Cape Canaveral Air Force Station, FL. This launch marked the largest ever payload for an Atlas V rocket.

Tech. Sgt. Adrian Jarrin, a flight engineer with the 920th Rescue Wing, Patrick Air Force Base, Fla., checks the time as he prepares to fly over Florida's Atlantic Coast to provide range clearing support for the Atlas V rocket launch July 19, 2013, Cape Canaveral Air Force Station, FL.



CIO's Network Tips



MALWARE PREVAILS IF SAILORS ALLOW IT

By Carlos Parter, Fleet Cyber Command

From: Computer

To: John Q. User

I am sorry my slow response is impeding your production this morning. It seems that I have been infected with a terrible virus or something. I can't seem to get going today and I am feeling quite sluggish. Hopefully, you or your friends will be able to help me find a cure.

**Signed,
Your Computer**

P.S. The good people at Navy Cyber Defense Operations Command have asked to have my hard drive shipped to them for forensic analysis, so I might not be available for a while.

What is malware?

Malicious software, or malware, is software used/created by attackers to interfere with computer operations, gather sensitive information or gain access to private computer networks. Malware often masquerades as a useful program (such as spyware removal tools; a type of program designed to prevent and detect unwanted spyware program installations) or is embedded into these useful programs.

Users are enticed into activating the malware without knowledge of the

attached harmful payload. Malware can appear in the form of code, scripts, active content and various forms of software. Some of the commonly known malware are computer viruses, worms, trojan horses and spyware. With the broader use of social media, attackers are expanding their methods of delivery.

Two examples of delivery methods are: posting links from a hijacked account to a user profile that redirects the unsuspected user to a malicious site and emailing graphic interchange formats (GIFS) and other attachments that are infected.

National Defense Magazine (November 2012), cited five major threats to National Security in the coming decade: biological weapons, nuclear weapons, cyber-attacks, climate change, and transnational crime. We categorize malware as a method of cyber-attack. The bad guys only need a small window of opportunity to exploit vulnerabilities, attack our networks, and steal sensitive information.

According to the Symantec Internet Security Threat Report released in May 2012, all advanced persistent threats rely on targeted attacks as their main delivery vehicle, using a variety of vectors such as drive-by-downloads,

SQL injection, malware, phishing and spam. The following highlights are provided:

- Symantec products recognized and blocked a total of over 5.5 billion malware attacks in 2011, an 81% increase over 2010.
- Web based attacks increased by 36% in the last year, with over 4,500 new attacks each day.
- 403 million new variants of malware were created in 2011, a 41% increase of 2010.
- SPAM volumes dropped by 13% from 2010 to 2011.
- 39% of malware attacks via email used a link to a web page.
- Mobile vulnerabilities continued to rise, with 315 discovered in 2011 (Smartphones, tablets, etc.).
- Of 49 companies examined in the US, average the per capita cost of a breach was \$194.00, and an average incident cost \$5.5 million in total.
- 39% of successful attacks/breaches were preventable and happened due to user negligence and 37% were caused by malicious or criminal attacks.
- Phishing attacks up to 0.33% or 1 in 298.0 of all email in 2011, from 0.23% or 1 in 442.1 of all email

“Network man says: beware, be cautious and be alert.”

in 2010.

- Note: Phishing attacks are increasingly targeted at regular users as opposed to flag officers and senior executives.

The Navy network and Navy personnel, at all levels, are primary targets for adversaries. Attackers are aggressively trying to exploit all vulnerabilities of our networks through various increasingly sophisticated means. Some are technical in nature (operating system patches, etc.) and others are not (poor security awareness, bad user behavior, etc.). It is also interesting to note that the majority of cyber criminals work only three days per week. They only work as hard as we make them!

As mentioned in the Symantec report, the attack footprint is not getting smaller and the recovery from cyber breaches can be quite expensive. Other hidden costs are initially missed because of secondary attacks. According to eHow Tech (2011): It is more difficult to quantify the

... continued on Page 25



cost of malware attacks. It is easy to calculate the cost of removing spyware from a network, but if the spyware has managed to capture some passwords, or even just part of a password, the spyware author can infiltrate a company's network and cause incalculable damage (secondary attacks). Many companies consider spyware the most serious threat. The McAfee report identifies the oil and gas industries as being the most vulnerable for what it terms "stealth infiltration." If you don't believe we are under attack, take a look at the statistics below (provided by the Navy Cyber Defense Operations Command (NCDOC)):

- In 2012 the NCDOC's Incident Management team received an average of 250 discovered/ reported cyber incidents every month.
- 55% of discovered/ reported cyber incidents were from malicious web links.
- 45% of the attacks targeted our afloat units.
- 22% of the attacks were on our Navy Marine Corps Intranet.
- 21% of the attacks were on our non-Enterprise networks.
- 9% of the attacks were on our ONE-NET networks.
- 4% of the attacks were on our BUMED networks.

Times have changed my friend. Prior to the computer age, the insider threat was our biggest risk. If I wanted

to protect my data, I locked it in a safe within a secure building and called it a day. Unfortunately or fortunately (depending on who's looking) we do not have the same luxury today. In the spirit of managing and sharing data more efficiently, we have exposed Navy networks and information to additional risks. However, through wise operational risk management, we can mitigate these risks. Just because the bad guys are banging on the door does not mean we have to let them in.

How do I protect myself and the Navy's mission?

Every day, you are the target of criminals and our nation's adversaries whether at work, deployed at sea, or at home. We are not expected to all be cyber security professionals. However, we are all required to know and use the fundamentals every day. You must be vigilant, cautious and informed when it comes to protecting our networks from malware. The following guidelines, found in the Fleet Cyber Command 'Navy Network Discipline Quick Tips User Guide', should assist in minimizing the risk of malware to our networks:

- Safeguard Information and Information Systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.
- Protect Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), and Classified information to prevent unauthorized access,

compromise, tampering, or exploitation of the information.

- Protect Password and Personal Identification Numbers (PIN) required for Logon authentication at the same classification as the highest classification of the information accessed.
- Protect authentication tokens (e.g., Common Access Cards (CAC), Alternate logon Token (ALT), SIPRNET PKI cards, National Security Systems (NSS) Tokens) at all times. Authentication Tokens shall not be left unattended at any time unless properly secured.
- Perform a Virus check on all programs and files prior to uploading onto any DON IT resource.
- Report all security incidents, including PII breaches, to your Command Information Assurance Manager (IAM) immediately in accordance with applicable procedures.
- Access ONLY the data, controlled information, software, hardware, and firmware for which you are authorized access, have a need-to-know, and have the appropriate security clearance.
- Assume only those roles and privileges for which you are authorized.
- Digitally sign and/or encrypt emails, as required .
- Follow appropriate email etiquette. Avoid "Reply To All".
- Employ sound operations security

measures IAW DOD, DON, Navy and Command directives.

- Get your FREE personal Anti-Virus and Firewall software for home use from your Command IAM.

References and Resources:

- Symantec Internet Security Threat Report
- Department of the Navy Cyber Crime Handbook
- Computer Viruses & How They Affect Our Economy
- Navy Network Discipline Quick Tips User Guide

Additional Resources:

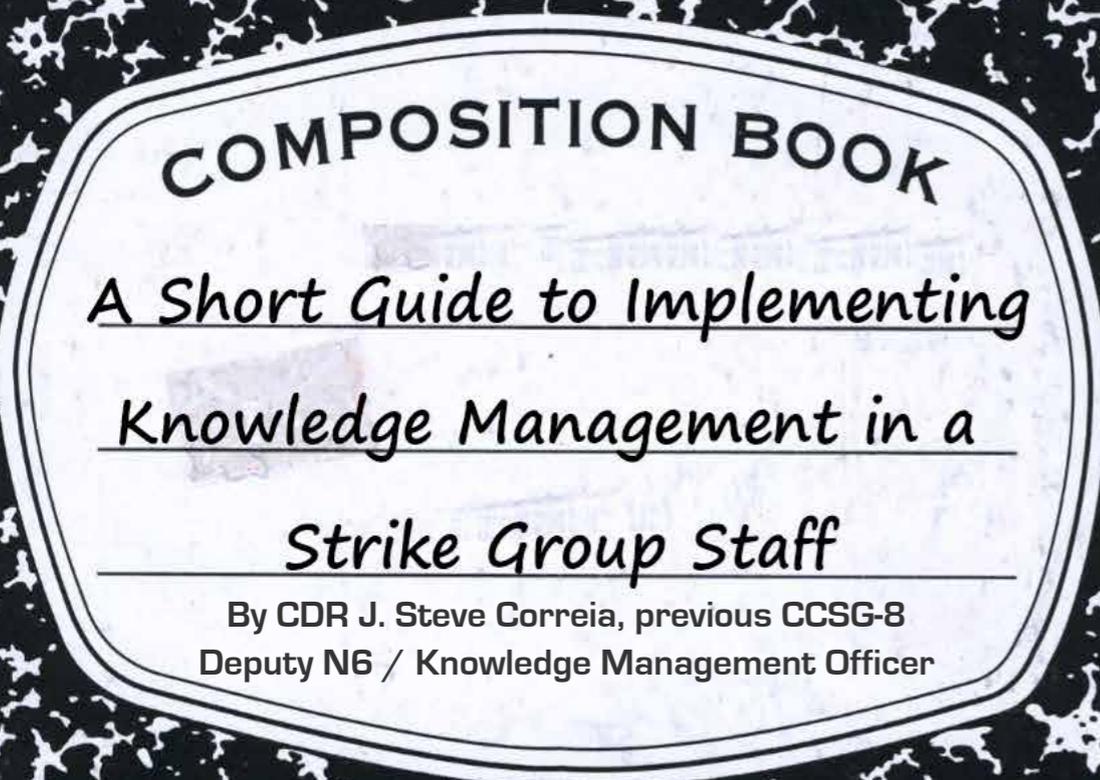
Navy Network Discipline message, NTD 06-11 (NETWARCOM 041745ZAUG2011)

Visit the Onguard Online website for related awareness information, training videos and games. ☞



"Stay safe my friends and remember Shipmates, don't let Shipmates abuse the Network!"





EDITOR'S NOTE: *This article is meant to be a guide to implementing Knowledge Management (KM) techniques within a strike group. My experience was on the CCSG-8 staff, initially deployed to the FIFTH Fleet AOR. My examples are from that experience; however, I believe these techniques can be used in a broader context.*

First things first: Never actually use the term Knowledge Management in your strike group. Our Navy's psyche has been damaged by the many unfunded, buzzword-laden programs of the past: TQL, the Revolution in Training, etc. In my opinion, it is best to use as few words as possible when implementing KM. In fact, if no one knows you are doing KM, all the better.

Perhaps when, in the not-so-distant future, your Admiral asks you, "Hey, Steve, what was that thing you did at the beginning of deployment that made the staff more efficient?" That would be the right time to break the news that you have been using KM. Learn and use the lexicon of the warfighter

Avoid geek-speak: save that for the KM forums and Information Dominance symposia. But I'm getting ahead of myself. Here are the KM change principles, according to my experience:

Principle #1: Find a quick win and implement it . . . fast. If you don't show value in the first 3 weeks of deployment or in the first few months of being aboard the staff, you will not likely

have a KM impact during your tour; however, you should go about your business quietly. Don't worry, I'm going to give you an easy quick win: your Strike Group (Collaboration at Sea) CaS Site. Chances are it has the following characteristics:

- Clutter, i.e. you can't find anything that you actually need. Worst of all, your Admiral, COS, N3 and Warfare Commanders can't find any of the information they need. Most CaS sites have too much clutter. Listen carefully, because this is important: More pages and more links do NOT make a better site. For you math types: more ≠ better. The CaS winner is not the one with the most links. More links likely only mean that you have more outdated and marginally useful information posted on your CaS site.
- The useful information is buried on some page 8 clicks away. It should not take any user more than 2 or 3 clicks to get to the information that they need or want. Your CaS site does NOT have to look like your command structure. Each N-code and unit does not need their own page. In fact, you should boil down the number of pages on your site to the bare logical minimum. Under our control the CCSG-8 and

... continued on Page 27



CTF-50 sites had 3 pages on the entire site: (1) The home page which has all the daily briefs, i.e. Commander's brief, Weather brief, Intel Brief; the current operations briefs, i.e. port visits, transits, exercises, etc.; and the Strike Group Headlines. (More on headlines later.) (2) An archive page with all the recent exercise and operation briefs. (3) An extensive links page.

- Libraries. Your libraries are the wild, wild west. You likely have 14 of them. Some of the information is likely from 2006 and was posted by someone that is now out of the Navy. Ask yourself this question: Is the Warfare Commander's Brief from 2006 useful? If the answer is no delete it. I realize this may cause you some angst. We live in a world that no one wants to delete anything. After all, information is power and PowerPoint briefs are information. Information Management (IM) demands that you delete! Our share drives and CaS sites are filling up and we must take action! If not the KM, then who, faithful reader? Who? Here is a good rule on deleting: If it's a brief for an exercise or operation, keep it. It may be useful to someone during the next spiral of the exercise or

operation. You probably only have to keep the main briefs from the last two exercises or operations of that series. For daily or weekly products, only keep the last few. No one will need an AirPlan or WCCB brief from the last deployment. They will be making new ones each day already. If you are the worrying type, have your ITs copy the briefs on an external drive and see how many people come looking for the information. I tried this experience and my

- Headlines. This wasn't my idea. My Admiral

directed me to do this one, but I think it worked well and I want to share it because it works. Make a section on your CaS homepage that gives the "headlines" for your strike group. This works particularly well when doing operations, i.e. in FIFTH Fleet. Your units and Intel shop are likely making storyboards for the major events in the strike group: DDG captures pirates, Air Strike eliminates enemy fighters, etc. Post that slide like a news stories

"What is also true is that you will never be able to do any KM if you have not handled IM. IM is a prerequisite to KM."

to that section. The idea here is to post both the successes and "others". This will allow your group and those that follow insight to the successes and challenges faced, i.e. knowledge retention. I maintained control of what was posted in consultation with the N3. More on site control later.

- If possible use an operational site for the area you are working in. For example, CCSG-8 assumed the duties as CTF-50. There happens to be a CTF-50 site.

It was not being used. We used it. That site was all operations. If there is no such site

for your assigned TF duties, your CCSG site will do or you can have the CaS help desk create a site (that is part of what they do). So fix your CaS site. I hear you asking, "but Steve, that is more of an information management function and not really KM." That is true reader. Very true. What is also true is that you will never be able to do any KM if you have not handled IM. IM is a prerequisite to KM. IM is the base of the pyramid. If you are not brilliant on the basics your program will never get off the ground.

You will be like the NFL team with the best quarterback in the league and no offensive line. You will not win many games if you don't handle the basics.

Principle #2: Identify the key people in the organization and find a way to convince them that the work you are doing is of benefit to them and the organization. The key people in an organization are NOT always the people at the head of a N-code. Organizations are complex. Sometimes the key people are obvious: the Admiral, the COS, the N3, but sometimes they are not.

"Influencers" inside the organization wield a significant amount of influence over the group and they are NOT always at the top of the organization. It could be a Chief, an OS2, or a LT. Finding the influencers in an organization takes some work and observation

Here are two hints to finding the influencers: (1) They get things done. When people want things done they go to these people. They are the IT2 that the COS wants in his office to fix his profile issue. (2) These people have a lot of connections to others in the organization.

People come to talk and see them often. Why do you care about influencers? You will not be able to implement change without them. If you convince them, you can change



. . . continued from Page 27

the organization with less work. It's like organizational kung-fu, faithful reader. See the book Tipping Point by Malcolm Gladwell for more on this. Here is another good resource: <http://www.netform.com/default.htm>

Principle #3: Get people to use your CaS site. If people are emailing final drafts of briefs around your Strike Group because it's "too hard to post" or "I can never find it on the site" you have a problem. So how do you get people to use your site? Answer: execute on principles #1 and #2. Make your site easy to use and work with the emailers to get there information posted. Make posting it easy or train a few Sailors to do it. If you can get the people that do the daily briefs to do this, the rest will likely fall in line.

When I arrived at CCSG-8, the following is a sampling of the briefs that were being emailed on and off the ship on a daily basis: the Intel Brief, the Weather brief (twice a day), and the AirPlan. Of these, the Intel brief was the largest, averaging 8MB in size. Do you know what an 8MB brief does to a DDG's communications pipe? It's not pretty. I approached the N2 first. His response: No thanks. We are happy just emailing it. We have reasons A, B, and C to email it. We are not interested. Now what? How about the AirPlan?

IKE's Strike department was

producing the plan and they were already posting to CaS in addition to emailing it. I asked the LT that was emailing the plan out to make one small change. Instead of emailing the plan, email out a link to the plan on the CaS site. As the KM you should have a thorough understanding of how CaS replicates and the difference between a local (on-ship link) and a shore-side link

You should provide BOTH links with any email directing users to a file on CaS. The reason that you should do this is because your users do NOT understand the replication process and the first time they click on a link that does

not work or that takes 10 minutes to load, you have lost them and briefs will be emailed instead. In my case emailing the AirPlan link was a success. The N2 saw that it worked and became interested. I was able to convince the new N2 and his deputy to use a link.

The weather guys followed soon after. I or one of my CaS administrators started posting all the operational and exercise briefs to the site. Our N3 started emailing the links to people instead of the briefs themselves Soon he started simply directing people to the site. Several people on the

N3 commented on how much useful information was available on the site: all our current or soon-to-execute operations. Our Battle watches would go to the site to get the briefs. We hit the tipping point. Everyone wanted their briefs posted to the site and no one was emailing their briefs around 8 a.m..

Principle #4: Control the CaS site. This may seem obvious or mundane, but it's important. So here is the trade-off: you want people to post because

your posters will help you keep the most up-to-date information on the site, but the more

posters you have the more chaotic your site will become.

We've already covered why a chaotic site is bad. You will have to find the right balance. I preferred keeping tighter control over my site. I'm sure it has nothing to do with my type A personality.

Here is how I found balance: I trained the "daily posters" on how and where to post. They posted the information as it was released but they posted it in a pre-determined place. The result: timely information that fit into the overall design of the site.

Principle #5: Participate heavily in the battle rhythm of your staff. You should be on the watchbill working toward an operational qualification and participating in at least one planning meeting in the staff's battle rhythm: a daily working group or the Admiral's daily brief or both.

The reason is clear: If you are in the battle rhythm you spot the issues with information and knowledge flows. Nothing drives home that the BWC isn't getting the information she needs to do her job, like being there.

Well, faithful reader, those are the basics. If you can get this far, you have laid the groundwork for a great KM environment on your staff. You have earned the respect of your staff. You have made the influencers part of your team.

The staff in general sees some use in what you are doing. Once you have respect and trust, your other initiatives will meet with less resistance. Now you can make some real change for the better. Good luck. ✂

"The reason is clear: If you are in the battle rhythm you spot the issues with information and knowledge flows."





Safari
BOOKS ONLINE

You Name It – You Can Learn It OnLine & for FREE

Safari Books Online, A treasure trove of information

By Denise Nason Kiley, Safari - Navy Resource Liaison

A Sailor recently told me he read about Safari Books Online in the Spring 2011 edition of InfoDOMAIN and he needed some additional pertinent information – “How do I find DoD access to Safari?”

As a representative of Safari Books Online, I can help you gain access to a product that contains approximately 33,000 technical books, training videos, business building manuals and much more.

Are you studying to be a systems administrator? Do you need to complete certifications to meet a job requirement to enhance your career or a personal goal? Do you know how to build a website? Maybe you want to buy your first house or you need to brush up on algebra or calculus? Perhaps you’ve just discovered your inner shutterbug but don’t know much more about that new digital camera past the on/off button. Or there’s a job interview on the horizon you want to nail ... or you want to do more than dream about retirement; you want to prepare for it.

If any of these apply to you, Safari Books Online has resources that will help...and you can access the content from your computer, phone, iPad, or other mobile device and let the learning begin!

WHAT IS Safari Books Online?

Safari Books Online, among other things, is an online technical book and video library that was selected by the DoD librarians jointly, paid for with Morale, Welfare and Recreation (MWR) funding, and is available to all branches of the service. It’s a venue open to active duty, retirees, DoD civilians, most contractors ... basically those who either have a ‘.mil’ email address and/or who are registered in the

Defense Enrollment Eligibility Reporting System (DEERS).

The content covers more than 90 percent of the top technology books published today and used widely by government, defense and intelligence agencies. With more than 33,000 books and 6,000+ hours of training and instructional videos to keep certifications up to date, Safari Books Online is for on-the-go learning and serves as a “must have” technical library.

And it’s mobile too. Safari To Go is a free app available from the Apple App Store, Google Play or Blackberry World designed specifically to use on iOS,

Android and Blackberry devices. You can cache up to three books in your Offline Bookbag to read at your leisure, create bookmarks while reading and manage your favorite content using personalized lists.

You can also access the

entire Safari library on any device for ONLINE reading in addition to offline caching via the free apps.

This Safari content saves so much money by allowing you access to these resources without having to buy costly books and it’s always up to date. And Safari adds over 100 books per month, usually providing access to new releases before you can purchase them in bookstores. So return to the site often to see what’s been added.

Visit the Safari website <http://www.safaribooksonline.com/> or the Library Section of your Knowledge Portal (AKO, NKO, ...) for more information about this product and see the full line of available titles.

“I am truly enjoying access to the Safari Library. The Safari site provides the most empowering knowledge base I have ever had. ... My “brain is keen but my pocketbook lean”, and I would not have been able to do what I am doing without your help.”

Former Chair of the Computer Science Department and Professor Emeritus, U.S. Naval Academy

... continued on Page 30



. . . continued from Page 29

If you have any questions or feedback for me, Denise Nason Kiley, I can be reached at dkiley@safaribooksonline.com. You can also request a site visit to your base or installation, where possible, and provide Safari training. ✂

HOW TO FIND Safari Books Online - *The path to Safari is still a mystery to most. Here is a simple set of instructions, paths from the Knowledge Portals, to help eligible users to find Safari.*

Air Force personnel & family members:

[Air Force Portal https://www.my.af.mil/faf/FAF/fafHome.jsp](https://www.my.af.mil/faf/FAF/fafHome.jsp)

1. Click on Library Tab.
2. Mid page down the page under EBooks and Downloadable Audiobooks.
3. Click on Safari logo to register
4. Path AF Portal > Library tab > EBooks and Downloadable Audiobooks > Safari

Navy & Marine Corps personnel & family members:

[Navy Knowledge Online https://www.nko.navy.mil/portal/home/](https://www.nko.navy.mil/portal/home/)

1. NKO, Library main page - "reference" on top right of home page click on Reference "Navy-E library"
2. On left hand side click on E-library - Computer and IT
3. Click on Safari logo to register
4. Path NKO - Reference > E-Library - Computers / IT - Safari

Also -- it is listed in Reference > E-Library - Audio & EBooks

Army personnel & family members:

[Army Knowledge Online https://akologin.us.army.mil](https://akologin.us.army.mil)

1. Go to Self Service
2. Choose My Library
3. Go to list of databases
4. Choose Safari and registerPath - AKO > Self Service > My Library > Databases > Safari



Safari To Go!

Get Safari Books Online on your iPhone, iPad, Blackberry, Android phone or Android tablet.

Safari To Go is a perfect combination of the powerful Safari Books Online platform and the portability of your favorite handheld devices. With Safari To Go, you can search for information in a book or video and have on-the-go access to your lists, bookmarks and recent books or videos—anytime, anywhere.

Safari To Go is not just any mobile-ready application; it was designed specifically for use on iOS, Android & Blackberry devices. Safari To Go capitalizes on the native functionality and convenience of these devices to give you the best of the core features and tools that Safari Books Online has to offer. And, it's free!

With Safari To Go you can:

- Pick up where you left off from any Safari Books Online reading platform
- Cache up to 3 books in your Offline Bookbag to read offline
- Create bookmarks while reading
- Manage your favorite content using personalized lists
- Synchronize recent views, bookmarks and lists across all of your readers
- Use 3G or 4G for fast load times

Safari To Go Is Free
Download it now from the
Apple App Store, Google Play
or Blackberry World and
start using it right away!



GET SAFARI BOOKS ONLINE TODAY!



Safari Books Online, LLC is a joint venture between O'Reilly Media, Inc. and Pearson Education, Inc.
© 2013 Safari Books Online. All rights reserved.

safaribooksonline.com



Sailors Remember Fallen Shipmates on Memorial Day

Story & Photos by CTN3
Zachary Barnes, NIOC Hawaii

Memorial Day throughout the United States is a day for remembrance and tribute for those who have gone before us. Our late fathers, mothers, friends and colleagues are in our hearts and this day gives us pause to stop and consider their contribution and impact to our lives, both personally and nationally. Hawaii's military history and Asian culture uniquely enable us to honor our shipmates. Military honor in combination with the filial piety of Japanese heritage make for a truly memorable Memorial Day.

In 1999, the head of the Shinnyo-en Buddhist Order, Shinso Ito, officiated the inaugural Lantern Floating Hawaii ceremony in a small lagoon on the south shore of Oahu. This service is considered to be one of the greatest Memorial Day spectacles around the world, and is rated by Fox News as number one of the top ten moving Memorial Day destinations, ahead of events held at Colonial Williamsburg, VA, Gettysburg, PA and the Arlington National Cemetery in Washington, DC. More than ten thousand people gathered on the shore of Ala Moana Beach Park to participate in the ceremony.

Lantern Floating Hawaii exemplifies the feeling of deeply mournful, yet incredibly proud, respect for our national heroes, which all veterans share. The ritual pays respect to lost loved ones with prayers and messages written on rice paper surrounding a candle on small floating lanterns set to sea near dusk. Soldiers, Sailors, and civilians alike remember their loved ones who sacrificed their lives at war.

This year more than 6,000 lanterns were set adrift in memoriam. A sight truly moving, each one a selfless thought of someone else, yet together, a profound statement to the departed: "You are not forgotten."

"I thought the event was beautiful. 'Many Rivers, One Ocean' was a great theme and it showed in the atmosphere and diversity of the thousands who gathered," says NIOC Hawaii Sailor, CTR1 Jeremy Gottschalk.

Taiko drummers beat a prayer for peace before the six "Parent Lanterns" were set adrift, carrying the prayers for victims of war, natural and human disasters, famine and disease with hope of encouraging harmony worldwide.

Community leaders, Shinso Ito, and honoraries spoke, enriching the experience with their thoughts of their ancestors and heroes.

Among the speakers during the ceremony was former Army sergeant of the 804th Drum and Bugle Corps and World War II survivor of the attack of Pearl Harbor, Allen Bodenlos, who was present at the ceremony to honor his best friend and fallen Sailor, Clyde Williams. Upon his lantern he simply inscribed, "To my best friend," a quiet bond of brotherhood and love for someone who impacted his life so profoundly more than 72 years ago.

Bodenlos was only on the island for one day in 1941 before all 26 other members of his band were lost in the attack. He was just across from the harbor when the attack began, in the process of returning to his battalion at Schofield. "I was right across from the

Arizona when it blew up, I watched the Oklahoma roll over, saw the West Virginia and California go down, and the Nevada get under way. Then we dove in a ditch as the Japanese pilots flew just overhead."

"It's my first duty when I get here, to go to the Arizona, and pay my respects," Bodenlos said.

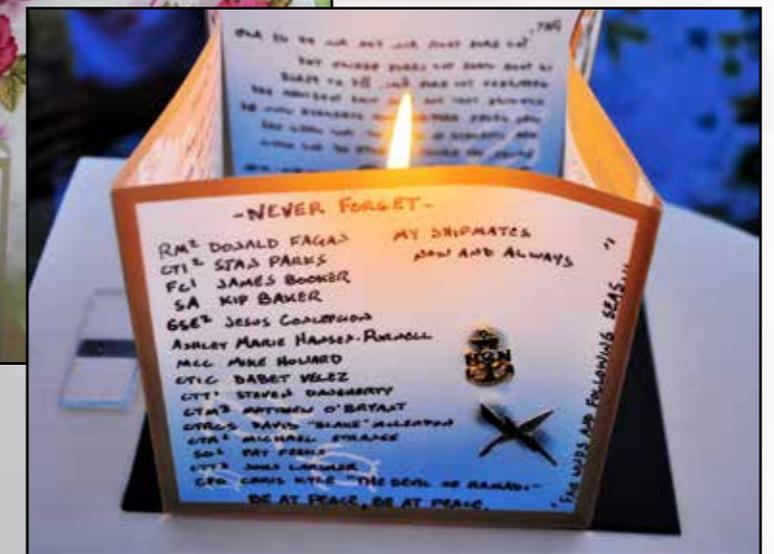
Bodenlos has volunteered in San Diego at the VA Hospital for the last 20 years, and traveled to share his experience with more than 100,000 high schools, colleges and at events such as this.

"Allen is a national treasure," says David Atkins, Bodenlos' "adopted" family while he's on the island. "He has dedicated his life to public service."

Along with Bodenlos, Soldiers, Sailors, Marines, and Airmen also dutifully honor those who have died in the name of the United States. Commanding



(Left) Pearl Harbor survivor, Allen Bodenlos, prepares to add his lantern to the 14th Annual Lantern Floating Hawaii ceremony. (Below) The lantern ritual pays respect to lost loved ones with prayers and messages written on rice paper surrounding a candle.



... continued on Page 32



. . . continued from Page 31

Officer, Naval Information Operations Command (NIOC) Hawaii, Justin Kershaw set out to honor every Sailor who had died in the line of duty during the current War on Terror. The NIOC Diversity Counsel, lead by ENS Kyle Crump, sponsored all 229 Sailors who have fallen during current military engagements. NIOC Sailors were given the opportunity to choose from the list of names and float a lantern in commemoration of their sacrifice and contribution to the Navy's "Global Force for Good".

Joining Gottschalk to pay tribute to their country and their predecessors were CTN1 Marissa Viaene, CTN3 Darlin Paz, and CTR3 David Polsdorfer.

Viaene, who was in attendance at the event with her sister and friend, sponsored five Sailors. On each of their lanterns, she wrote a quote from past and

present presidents, an homage to the idea of freedom and liberty that they gave their lives for.

Viaene acknowledged the dedication and sacrifice of those overseas by researching their obituaries and familiarizing herself with their stories. "I have a lot of respect for these men and women. When I signed the papers to join the Navy, I understood that I could die [too]," said Viaene.

A common theme among the service members who attended the lantern floating was an understanding and acceptance of the implications of war, and their own service as a Sailor. "I decided to participate because of a deployment I was on in 2011. There was a huge list on a wall at Fort Dix of Sailors who died in Afghanistan. Being [at the ceremony] made me thankful for not being one of those lights," said Polsdorfer.

Polsdorfer sponsored two fallen Sailors at the lantern ceremony. Michael Gray died in 2004, and Sean Brazas in 2012. They were both the same rank as Polsdorfer. "Seeing [Allen Bodenlos] made me wish I knew both of them personally; it made me think of the people remembering them on that day too -- their families, friends and shipmates," he said.

Not only were the lanterns a vessel of memory and honor, they signified a more tangible means of acceptance for those left behind to mourn the losses. Paz notes how calm she felt, setting her lantern adrift. "It feels like we're putting them at peace. I feel thankful for each person who has contributed their life, especially the Veterans. The lantern ceremony was the perfect way to do it." ✂

NIOC Hawaii Sailors Join Local High School JROTC for Annual Cyber Patriots Program

Story & Photo by CTN3 Zachary Barnes, NIOC Hawaii

Four local Navy Intelligence Operations Command (NIOC) Hawaii Sailors have dedicated their time and knowledge of computer security to local high schools. Their time and mentorship are sparking the fire that will create tomorrow's future cyber warriors.

Cryptologic Technician Networks (CTN) 1st Class Domonic Richmond, CTN1 Darryl Schneider, CTN2 Jacob Cruz and CTN3 Kirk Moeller volunteered to lead a small team from the Mililani High School Junior Reserve Officers' Training Corps (JROTC) to compete in Cyber Patriots. Cyber Patriots is a national-level competition where JROTC cadets around the U.S. compete in different events involving computer network defense (CND). Cadets compete on

the state level before moving on to the national competition in Washington, D.C.

Areas of focus include good network administration postures, basic network topology, good password policy, securing vulnerable services and identifying unknown or unwanted connections from intruders.

Richmond talked about the competition. "I love working with kids. They want to be there, and everything we went over was fun. They stay interested."

"We have a rough idea of what we need to know for the event. For example, they have to lock down a Windows 2008 server," Richmond said.

"They are given an image that has been compromised and directions for

what the judges expect to be secured. They are asked to remove a backdoor, get rid of personally identifiable information (PII) and unauthorized media, while still allowing it to function as it was intended," added Moeller.

Richmond and his shipmates imparted their expertise to the cadets, enabling them to move on and achieve outstanding results in



CTN3 Kirk Moeller and CTN1 Darryl Schneider . . . two of four members at Mililani High School's JROTC program.

several categories, reaching second

. . . continued on Page 33



... continued from Page 32

place overall in the state. To mark their success, CAPT Justin Kershaw, commanding officer of NIOC Hawaii, presented each of the cadets with a

command coin for their efforts and execution during Cyber Patriot.

“The cadets were honored to be awarded by both the Air Force Academy and the CO. Their parents

were also very grateful to the Navy for taking time to mentor their kids,” said Richmond. The cadets, with the help of the Sailors, established a permanent cyber battalion within the JROTC. They

formed this new cell with the goal of competing and winning at the next Cyber Patriot event. ✂

NIOC Hawaii: Saving Lives in Paradise

By NIOC Hawaii PA Team

There’s something special about NIOC Hawaii, and not just the gorgeous weather year-round. Sailors at this command have been going above and beyond the call of duty, taking swift and heroic actions that have proven to save lives. Though each situation the Sailors found themselves in were drastically different in nature, the Sailors all maintained their composure while stepping up in times of dire need. These Sailors wholly embody the Navy’s core values of Honor, Courage, and Commitment, as you can see in their stories below.

Fire in the Barracks

By ENS Julio Seanez

In the afternoon on January 25, CTI3 Alisa Morrow rushed into a burning barracks building and rescued a baby. Morrow and her fellow Sailors had scheduled a BBQ to celebrate their transition into the newly constructed E-4 barracks at NCTAMS. Shortly after 4:30 p.m., the fire alarm in the barracks went off. “I thought it was test,” said Morrow. As people were exiting the building, reports came that there was smoke coming from one of the rooms. Upon hearing these claims Morrow ran inside to investigate. “At first, I thought someone had burned popcorn or something but when I busted the door open and saw how much smoke there was I knew it was a bigger deal.”

Thinking that someone could be in trouble,

Morrow covered her mouth with her shirt and entered the room. “The fire was in the kitchen, I grabbed an extinguisher and put it out but there was still lots of smoke. No one was in the room though, as I was leaving the building I heard a baby somewhere in the lobby. When I found her I picked her up and ran outside.” The baby belonged to a barracks petty officer who was busy clearing the rest of the building. When later questioned, what compelled her to enter the building in the first place Morrow replied “I just wanted to see a fire!”

Morrow was awarded the Navy and Marine Corps Achievement medal for her heroic actions. ✂

Down in the Ala Wai

By CTI2 Ron J. Garza

In the early hours of the night of December 12, 2012 CTT2 Meghan King and CTT1 Benjamin Northcutt were out walking near the Ala Wai canal, in the Waikiki area, when they noticed an elderly pedestrian shouting for help and pointing into the canal’s waters. An unknown man was drifting facedown, unmoving. After noticing that the man was unresponsive to the shouts of bystanders, Northcutt jumped into the canal and began to pull him to the concrete embankment.

“I was stunned at first,” King recalled of her initial reaction to seeing a body floating in the water, but “snapped out of it when [Northcutt] jumped into the water.”

As Northcutt moved towards the bank, he performed the Heimlich maneuver in an attempt to clear canal water from the man’s stomach and lungs, while shouting for help to pull them both from the water. “I had to do something while I was down there, since the sidewalk was about here,” Northcutt stated, gesturing to a spot about a foot above his head.

The sidewalk embankment next to the Ala Wai canal, on the Waikiki side, is positioned several feet higher than that of the opposing bank, to prevent possible floodwaters spilling over into the streets of Waikiki. As such, it was difficult for Northcutt to find enough leverage to pull the both of them out of the canal, while being assisted by King and another bystander.

Once the man was safely out of the water and on the sidewalk, the two Sailors began basic first aid; King checked for an active pulse and regular airflow, and noting a lack of response and breathing, Northcutt performed CPR. After nearly a minute, the man resuscitated, coughing and clearing brackish Ala Wai water from his lungs, and soon was transported by paramedics to a local medical facility for further treatment.

The entire event took place over the course of a brief five minutes.

The Ala Wai canal is known for its polluted state and lack of moving current, with city officials warning the public to refrain from fishing or swimming in

... continued on Page 34



... continued from Page 33

the water due to health concerns. It is unclear how long the man remained in the water before King and Northcutt were alerted and acted as rescuers. However, Northcutt was informed by the paramedics that had he not performed the initial abdominal thrusts in the water, “[the man] would’ve been dead in a minute.”

Four days later, Roland Libby contacted CAPT Justin Kershaw, NIOC Hawaii Commanding Officer, via email.

Libby wanted to meet with the Sailors who saved his son, Ryan Libby. The Libbys, Roland and Sandra, graciously organized a Celebration of Life gathering to honor King and Northcutt for their actions; Northcutt was even invited, earlier in the day, to play a round of golf with Roland at the Mid-Pacific Country Club in Kailua. At the gathering Northcutt was awarded a Navy and Marine Corps Commendation Medal by Kershaw, and NIOC HI Executive Officer, CDR David Bandy. The award itself was pinned on by Sandra, in a fine gesture of appreciation. King received her award, a Navy and Marine Corps Achievement Medal, from the CO and XO.

Both King and Northcutt are brilliant examples of motivated actions under pressure; their deeds indicative of a calm and prevalent rationale in the face of danger. They should be proud of their willingness to put aside the self to help those in need, just as their command is proud of a great display of heroics. I salute them, and wish them luck and well being in their future endeavors. ✂

Heroes Among Us

By CTR2 Jeremy Wolfe

Most people do not wake up in the morning thinking they are going to save someone’s life. On December 9, 2012, HM2 Reynolds woke up anticipating his completion of the Honolulu Marathon. Reynolds was in the midst of the marathon

when he noticed a fellow runner on the group unresponsive. “[This is] what I’m qualified to do,” he said. “He wasn’t responsive right away so I had all the bystanders run and get ice and call an ambulance.”

The runner was suffering from a heatstroke. Reynolds put his training to immediate use as he struggled to get a response from the runner. “He barely spoke any English and what he did speak was very broken.” Once the man was responsive, Reynolds began to cool the runner’s body down, covering him in “ice from the water stations until an ambulance arrived”.

Community Involvement Reaps 3rd Award for NIOC Misawa Sailors

Navy Information Operations Command (NIOC) Misawa recently received the 2013 Nippon Zenkokai Association Good Conduct Award during a ceremony at the Sanshu-den Hall of Meiji Shrine here.

The Nippon Zenkokai Association is an independent non-profit organization committed to encouraging good conduct and the enhancement of warm mutual relationships amongst members of society. Every year they present awards to individuals or organizations that have made a significant contribution in their communities.

This is the third year NIOC Misawa was nominated and the third year they received the award, having been recognized in 2009 and 2011.

“We’re very proud to be a recipient again this year,” said CDR Sean Kelley, NIOC Misawa commanding officer. “Although it feels great to receive the award for our work in the community, it’s really not so much about the award, but rather just doing the right thing while living in Japan and working alongside the Japanese people.”

From the time Reynolds discovered the runner, to the arrival of the ambulance, Reynolds guessed it took almost an hour to get the man out. “It was probably the longest hour of my life,” Reynolds described. He never heard from the man, and did not receive and update from the marathon committee, but asked if he would do anything differently he simply stated, “if this kind of situation ever happened to me again, I’d do it all over again.” ✂



CTR1 Joshua Conner receives the Zenkokai good conduct citation on behalf of NIOC Misawa Sailors. (Photo by MC1 Barry A. Riley)

NIOC Misawa Sailors have a long history of supporting the local community that dates back to the 1960s. They have longstanding relationships in northern Japan, including community service projects with the Akebono Orphanage and teaching English to Japanese students through the Jido-Kan program. They also conduct annual events with students from the town of Gonohe including weekend host-family exchanges, and organizing a Gonohe Sports Day, in which Sailors and their families visit the town for a day of traditional, and not so traditional, sporting events. ✂



Local Officer Receives 2013 BIG Award

Story & Photo by MC2(SW) Jacob D. Galito, NAVCYBERFOR Public Affairs



CDR Bobby L. Hand, operations officer, NCTAMS LANT

CDR Bobby L. Hand Jr., operations officer assigned to Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT), recently received the 2013 Blacks in Government (BIG) Meritorious Service Award August 20, 2013.

The BIG Meritorious Service Award honors military members and Department of Defense (DoD) civilian employees, men and women, who have supported the DoD mission, overseas contingency operations, or whose attributes best epitomized the qualities and core values of their respective Military Service or other DoD Component.

“Receiving this award is a great and unexpected honor,” said Hand.

Hand, a Fort Gordon, GA native, received his Bachelor of Arts from Morehouse College in 1995. He received his commission to Ensign through the Reserve Officer Training Corps (ROTC) scholarship program and follow-on training at the Surface Warfare Officers

School and Engineering School in Newport, RI.

In 2012, he was designated as an Information Dominance Warfare Officer and was selected to serve in his present billet as operations officer, NCTAMS LANT.

Hand is a graduate of Navy Legal Officer School, Commanding Officer/Executive Officer Leadership Training, and Command, Control, Communications, Computers, and Intelligence Systems Engineering/ Communications Management School and holds a Master of Science in Information Technology Management from Webster University.

“I feel humbled,” said Hand. “There are so many more candidates much more qualified and deserving than myself.”

“I’m thankful for all of the senior enlisted leadership for being a part of my life since I was a midshipman,” said Hand. “I wouldn’t be here if not by their example and their not-so-gentle prodding.”

“His character, integrity,

intelligence and exceptional leadership inspire all who work with him,” said CAPT Danelle Barrett, commanding officer, NCTAMS LANT. “His ability to motivate others to excel and unmatched dedication to service to the Navy and the nation make him the ideal candidate for this award Barrett said.”

BIG was established in 1975 as an organization for African Americans in public service to organize around issues of mutual concern that could use their collective strength to confront workplace and community issues. BIG’s goals are to promote equity in all aspects of American life, excellence in public service, and opportunity for all Americans.



Misawa Sailor Earns 'On-the-Roof Gang' Award

NIOC Misawa Japan's Public Affairs Team

Fleet Cyber Command named Master Chief Cryptologic Technician Collection Matt Bouchard as the 2012 recipient of the "On-the-Roof Gang" (OTRG) Award.

The award, which is named after the original Navy cryptologists who trained in a specially constructed block house on the roof of the old Navy Department building in Washington DC, is given to a Sailor and Marine who best exemplify sustained superior performance and significant contributions to naval cryptology.

Bouchard, who originally hails from Fairfield, ME, currently serves on board Navy Information Operations Command (NIOC) Misawa, which is located on board Naval Air Facility Misawa in northern Japan.

"Please understand this," said LCDR Bryan Luallen, NIOC Misawa executive officer, and a native of Pensacola, FL. "The OTRG award is a cryptologic lifetime achievement award, not something awarded for a specific task. I know Master Chief Bouchard very well and I consider him to be a leader of the highest caliber, my mentor as executive officer and my friend. When he offers me counsel, his words do not go unheeded."

Unfortunately, Bouchard will not be able to attend

the awards ceremony later this month in Savannah, GA, but he said it was a major honor to even be nominated for an award named after such prestigious company.

"Since this award commemorates the founding fathers of naval cryptology, I am proud to be able to shed light on these trailblazers who made it possible for us to do the things we do today," said Bouchard, a 28-year Navy veteran.

"In the beginning, it was about learning my trade from the technical experts," he said. "I was lucky enough to learn from some of the best cryptologists in the business. And as I advanced through the ranks, my role changed from operator to leader. I think I was equally blessed to lead some of the most motivated and dedicated Sailors in the Navy."

Bouchard's OTRG Award will arrive in Misawa via mail, and NIOC Misawa will conduct a modest ceremony to congratulate him on his accomplishment.

Bouchard has recently accepted his final set of orders, and will transfer to NIOC Georgia in August, where he'll retire after completing 30 years of service.

Since 1988, the U.S. Naval Cryptologic Veteran's Association has sponsored the annual OTRG Awards, which recognizes service members' sustained superior performance and significant contributions toward naval cryptology for an extended period of time. ✂

"I was lucky enough to learn from some of the best cryptologists in the business. And as I advanced through the ranks, my role changed from operator to leader. I think I was equally blessed to lead some of the most motivated and dedicated Sailors in the Navy."



CTRCM Matt Bouchard

ON-THE-ROOF GANG FACTS

- On Oct. 1, 1928, the first class for enlisted Navy and Marine Corps Radio intercept operators, the "On the Roof Gang," began training in a unique classroom on the roof of the old Navy Department Building in Washington, DC.
- The "On the Roof Gang" was a school for radio-men and cryptologists who would go on to deploy on ships and at overseas bases and monitor foreign communications to monitor the movements, operations and intercept the message traffic of foreign navies.
- By the time the school closed in 1941, 150 Navy and 26 Marines had been trained.



Drive & Dedication Net OIC VADM Mayo Award

By George Bieber,
NAVCYBERFOR Public Affairs

LCDR Robert D. Matthias of Navy Cyber Forces Detachment San Diego was the recent recipient of the 2012 VADM Richard W. Mayo award. The prestigious Mayo Award, named for the first commander of the Naval Network Warfare Command, is presented annually to an Information Professional officer who demonstrates vision, innovation and exceptional performance in Information Technology (IT), and operational Command, Control, Communications and Computers (C4).

As Navy Cyber Forces San Diego Detachment officer-in-charge and West Coast Cyber Security Inspection and Certification Program (CSICP) Stage II Team lead, Matthias led 13 CSICP training assessment visits (TAV) for ten afloat units and three shore commands. During that time, Matthias and his team identified more than 500 critical security improvements and provided on-site assistance in developing a more



(Above, far left) LCDR Matthias briefs members of the West Coast CSICP Stage II Program. (Right) Matthias poses with his wife Michelle following his commissioning on board the USS Midway Museum. (Official U.S. Navy Photos)

robust readiness program.

“NAVCYBERFOR DET San Diego does its best to cover Stage II TAVs for all commands in COMPACFLT AOR,” Matthias added. “The experience is incredible because we operate TAVs as though we are in a training environment. With the weight lifted off a publicized command score, leadership and Sailors alike are much more open sharing deficiencies and improving their cyber security posture.”

Matthias believes that everything accomplished under CSICP in the Pacific, could not have been done without DISA/FCC/NCF leadership, and all the supporting elements, working together as a team supporting the Fleet.

“From enablers, to taking on the role as warfighters in the cyber domain, I really love being in the IDC and getting a glimpse of what the future has in store,” he said.

Matthias was able to easily

translate threats, vulnerabilities, and mitigation plans to operational leadership and stress the importance of cyber security.

“Matthias is a leader who exemplifies the drive and dedication of the information professional community,” said CAPT Bennie Sanchez, NAVCYBERFOR Chief of Staff. “He is committed to working with the Fleet and focused on improving our Navy’s maneuver capability and agility in a warfare area that is constantly evolving.”

The selection process was understandably competitive, with the recipient chosen from a field of outstanding candidates. Runners-up included LCDR Pablo Breuer, assigned to U.S. Cyber Command and LCDR Victor Taylor, assigned to Task Force 70.

Last year, NCF DET SD was the only one out of 145 commands/units/detachments authorized to train,



board, and pin Enlisted Information Dominance Warfare Specialists (EIDWS). OPNAV N2/N6 saw the disparity between IDC personnel with their assigned commands and opened the EIDWS Expansion Initiative.

“Through hard work and coordination of DET SD Chiefs and Sailors, we were able to include local Sailors into our program,” said Matthias. “We were the first to uphold the expansion by pinning Naval Beach Group Sailors and will continue to offer the opportunity for anyone in the San Diego area.”

The actual award will be presented at a later date and location to be determined. ✂



Newest Satellite Altimetry Sensor Launched

The SARAL (Satellite with ARGOS and AltiKa) mission carrying the newest ocean surface altimetry sensor, AltiKa, was successfully launched in February.

Global measurements from space-based radar altimetry sensors provide accurate, consistent, and repeated measurements of the shape of ocean's surface. Satellite altimetry measurements are critical to the Navy's ocean forecast systems, which support a number of fleet operations including ship safety and routing, and anti-submarine warfare.

The SARAL mission is a collaborative program between the French Space Agency (CNES) who built the radar altimetry sensor and the Indian Space Agency (ISRO) providing the PSLV launch vehicle. The new sensor, called AltiKa, is an innovative Ka-band altimeter designed to accurately measure the ocean's surface height and topography. The Naval Meteorology and Oceanography Command was able to secure access to this data at no cost to the Navy and has been working with NRL-Stennis and the Naval Oceanographic Office's (NAVOCEANO) Synoptic Data Division to ensure that NAVOCEANO's altimetry processing system is updated with algorithms to ingest and process the new AltiKa data stream for use in Navy forecast models. ✂



STENNIS SPACE CENTER, MS -- CDR Ron Shaw, Fleet Survey Team (FLTSURVTEAM) commanding officer, briefs ADM William E. Gortney, commander of U.S. Fleet Forces Command, on FLTSURVTEAM operations and capabilities during Gortney's recent visit to the Naval Meteorology and Oceanography Command and its subordinates at Stennis Space Center.

Navy Christens, Launches New Oceanographic Survey Ship

Accompanied by azure blue skies and a stiff breeze, the Navy recently christened and launched its newest oceanographic survey ship, USNS Maury (T-AGS 66), the last of its class, at VT Halter Marine's shipyard in Moss Point, MS, in a traditional Navy ceremony.

The 350-foot ship is named for CDR Matthew F. Maury, considered to be the father of oceanography, nicknamed the "Pathfinder of the Seas" and the

first superintendent of the U.S. Naval Observatory. Maury is 24 feet longer than its six sister ships to accommodate a 300 square-foot moon pool for easier deployment and retrieval of unmanned underwater vehicles.

RADM Jonathan White, Oceanographer and Navigator of the Navy and the principal speaker at the launch and christening, said the T-AGS ships are a reflection of

Matthew Maury, who he said, "led a transformation in our Navy."

The ship will be operated by the U.S. Military Sealift Command (MSC) for the Naval Meteorology and Oceanography Command (NMOC).

"If Matthew Fontaine Maury was here today to see this ship and to see the character of the people who built it, there is no doubt he would say, 'all's well,'" White said. ✂





BALBOA, Panama -- USNS Pathfinder (T-AGS 60) heads into port in Balboa, Panama, to conduct a hydrographic survey of the entrances to the Panama Canal. (Photo by Lee Kormandy)

NAVOCEANO & FST Breaks New Ground in Panama Survey

In February and March, Naval Oceanographic Office (NAVOCEANO) and Fleet Survey Team (FLTSURVTEAM) personnel conducted two new operations in conjunction with surveys of the north and south entrances to the Panama Canal.

The NAVOCEANO crew tested its new Core Deployment System, thanks to water depth of more than 4,000 meters during the transit to Florida at the conclusion of the survey operation.

In addition, the survey crew deployed and recovered a tide buoy, an operation many onboard had yet seen conducted.

“This hydrographic survey was unique in that the two commands worked installed on the Pearl Islands in January.

Kormondy describes his survey crew as a “nice cross-cut throughout NAVOCEANO,” and the survey operation itself as both a successfully completed top priority for the office and a great learning opportunity for the survey crew. ✂

USNO Dedicates New Correlator

The U.S. Naval Observatory (USNAVOBSEY) has gotten a new software-based correlator that will more efficiently process very long baseline interferometry (VLBI) data.

The new correlator became operational and USNAVOBSEY marked the occasion with a ceremony on Feb. 7 and named the equipment in honor of the late Dr. Gart Westerhout, a pioneer in radio astronomy who served as the observatory’s Scientific Director from 1977 to 1993. Dr. Westerhout died in October 2012.

The new correlator uses off-the-shelf hardware as compared to older generations of correlators, which required dedicated, custom-built, integrated circuits. The design change is more economical to build and maintain than past versions.

The Dr. Gart Westerhout VLBI Correlator Facility, used to reduce

VLBI data, is key to making a Celestial Reference Frame (CRF). The technique is to simultaneously collect radio signals from distant astronomical objects using widely separated radio telescopes. The data streams from the radio telescopes are processed through the correlator to determine the observed geometric orientation of the individual antennas, which allows for the very precise calculation of the Earth’s orientation in space and the sky positions of the radio sources. Earth orientation parameters (EOPs) are used by navigation systems (e.g. the Global Positioning System), communication systems, and by other space-observing systems. The CRF provides the fundamental reference frame for all astronomy, and is used for celestial navigation, precise pointing, the determination of the Earth’s orientation in space, and the orbits of Earth’s man-made satellites.

USNO began its involvement in VLBI during Dr. Westerhout’s tenure as Scientific Director. ✂

Flight Meteorologist Program

The Naval Oceanography Anti-Submarine Warfare Detachment (NAVOCEANASWDET), Whidbey Island, Wash., established the Flight Meteorologist Program (FMP).

The program gives Aerographer’s Mates and Oceanography Officers the opportunity to support tactical flights

on P-3s and gain first-hand experience on maritime patrol reconnaissance aircraft (MPRA).

Personnel must complete water survival training, qualify as naval air training and operating procedures observers, and fly a minimum of 60 hours to qualify. ✂



Naval Oceanographers Win International Humanitarian Award

By Jenni Ervin

A modeling capability developed by Naval Oceanographers at Stennis that predicts the likelihood of pirate attacks has received an international humanitarian award from Computerworld magazine.

IDG's Computerworld Honors Program selected the Naval Meteorology and Oceanography Command (NAVMETOCOM) as a 2013 Laureate in the field of Safety and Security for its development of the Pirate Attack Risk Surface (PARS). The Honors Program, founded in 1988, recognizes organizations and individuals who have used information technology to advance public welfare, benefit society and business, and change the world for the better.

"The men and women of Naval Operational Oceanography take great pride in this honor," said RDML Brian Brown, NAVMETOCOM commander. "Naval Operational Oceanography is a critical partner across the range of Department of Defense operations, and the development of PARS is one more way that we use our knowledge of the environment to ensure the safety and security of our operational forces and freedom of navigation on the high seas."

The PARS model produces a forecast of shipping vulnerability due to piracy at a certain latitude, longitude and time.

A few months before Somali pirates hijacked the U.S.-flagged MV Maersk Alabama in 2009, NMOC operators were asked to assist in the fight against piracy, which had been on the rise in the Somali Basin due to government instability in the region. Pirate attacks are a threat to the United States' national security and foreign policy, and they impact maritime safety, disrupt shipping and ultimately cost the world's economy billions of dollars annually.

Within two weeks, the command had developed the framework of the first-generation Piracy Performance Surface (PPS) model, which produced maps of probability of attack based on how environmental conditions influenced pirate small boat operations.

The success of the PPS model led to development of a more advanced anti-piracy model, the award-winning Pirate Attack Risk Surface (PARS). While the first-generation PPS primarily focused on environmental factors, PARS combines shipping information, environmental data, pirate locations, pirate operating procedures, and predicted pirate behaviors into a cohesive forecasting environment.

"PARS is groundbreaking," Brown said. "This is the only known Navy product that, instead of treating environmental data separately, fuses it with multidisciplinary information within a single model."

Computerworld judges evaluated the humanitarian benefits and measurable results of applying technology to meet a specific social or business need. NMOC's case study was selected from more than 700 nominations to become one of 268 Laureates from 29 countries.

Founded by International Data Group (IDG) in 1988, The Computerworld Honors Program is governed by the not-for-profit Computerworld Information Technology Awards Foundation. Computerworld Honors is the longest running global program to honor individuals and organizations that use information technology to promote positive social, economic and educational change. Additional information about the program and a Global Archive of past Laureate case studies, as well as oral histories of Leadership Award recipients can be found at the Computerworld Honors website. ✂

Australian Agreement Signed



STENNIS SPACE CENTER, MS -- RDML Brian Brown, NAVMETOCOM greets Martin Rutherford (right), Maritime Military Geospatial Information and Service Director of the Royal Australian Navy, after signing an agreement with the Australian Navy that has been 10 years in the making.

Dr. Ken Johnson Retires



WASHINGTON, D.C. -- Dr. Ken Johnson (left), Chief Scientist at the U.S. Naval Observatory, accepts a framed commemorative plaque at his office at the observatory from Dr. Bill Burnett, deputy commander and technical director of the Naval Meteorology and Oceanography Command, on the occasion of Johnson's retirement.





STENNIS SPACE CENTER, MS -- Tom Dunn (far right), Director of the Navy Department of Defense High Performance Computing Center at Stennis Space Center, briefs (l-r) retired astronaut Fred Haise ; Jerry Cook, Stennis Space Center Deputy Director; Rick Gilbrech, Stennis Space Center Director; and Ken Human, Stennis Space Center Associate Director; on the supercomputer and its three new systems. Dr. Bill Burnett (back), Deputy Commander and Technical Director of NAVMEOCCOM, also participated in the briefing. Haise was at the computer center because one of the three new systems was named for him as a former astronaut and one-time Navy pilot.

Apollo 13 Astronaut Visits Navy Super-computer Center

Apollo 13 astronaut and Mississippi native Fred Haise visited the Navy Department of Defense Supercomputing Resource Center (DSRC) at Stennis Space Center, MS, for a tour of the center's three new supercomputers – all named for NASA astronauts who have served in the Navy, including Haise who trained as a naval aviator.

The two other systems are named for retired CDR Susan Still Kilrain, a naval aviator and space shuttle pilot, and retired CAPT Eugene Cernan, a

naval aviator and the last man to step foot on the moon.

“Today, we are proud to recognize the contributions of an iconic American and native Mississippian,” said Dr. William H. Burnett, Deputy Commander and Technical Director of the Naval Meteorology and Oceanography Command at Stennis Space Center. “Just as Fred Haise has made a great impact on the state, the Navy and the nation so will the supercomputer named after him.”

The IBM iDataPlex systems were

installed in the fall of 2012 and became operational in January. The Navy DSRC is one of five Defense Department supercomputer centers that Navy, Army and Air Force scientists and researchers use to design tools and weapons systems that support DoD's global mission.

The new systems have tripled the supercomputing capability of the DSRC, already one of the most powerful supercomputer centers within the Defense Department.

“The fact that I'm here today was

dependent on computers,” Haise said. “We went to the moon on one tenth of a megabyte [of memory]. For four days we had no computer on board at all. That was the springboard of what is happening today in the computer world.”

The DSRC's current supercomputing capacity is 866 trillion floating point operations (teraflops) a second. One hundred high school students with handheld calculators would take nearly 317 years to perform the number of calculations a one teraflop-rated computer can accomplish in one second—and almost 275,000 years to perform what the new Navy DSRC supercomputers will be capable of every second. The DSRC is expected to increase its capacity to approximately 5,200 teraflops by 2016.

Haise, a native of Biloxi, MS, completed Navy flight training in 1954 and served as a U.S. Marine Corps fighter pilot and also served in the U.S. Air Force. His career with NASA spanned 20 years. He flew as the lunar module pilot for NASA's Apollo 13 space mission and as backup lunar module pilot for Apollo 8 and 11 and backup spacecraft commander for Apollo 16.

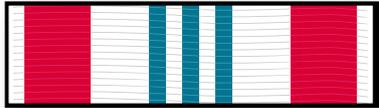
The Navy DSRC is a part of the Department of Defense High Performance Computing Modernization Program (HPMCP). For 19 years, the Navy DSRC has been recognized as one of the top 15 most capable supercomputing facilities in the world. ✕





LEGION OF MERIT

CAPT David Bondura, NIOC Texas
CAPT Robert Kelso, NAVCYBERFOR
CAPT Gregg Smith, NAVCYBERFOR
CAPT Andrew Stewart, FLTCYBERCOM
CAPT Timothy White, NIOC Maryland



DEFENSE MERITORIOUS SERVICE MEDAL

LCDR Audrey Adams, NIOC Hawaii
CTRC Puni Alefai, NIOC Hawaii
CTTC Stephen Boss, NIOC Colorado
CTRC Michael Brooks, US CENTCOM MacDill AFB
CTRC Danial Butts, NIOC Menwith Hill
CTTCS Bryan Cowan, NIOC Colorado
LCDR Johnnie Caver, NIOC Hawaii
CTRC Derek Erickson, NIOC Maryland
CTICS Michelle Evans, NIOC Maryland
CTTC Nolan Foltz, NIOC Colorado
LCDR Antonio Garcia, NIOC Maryland
ITCS Juston Geigley, NIOC Hawaii
LCDR Andrew Grabus, IV, NIOC Maryland
CTNC Kimberley Hanscom, NIOC Maryland
CTRC Erika Haws, NIOC Misawa
CTTC Martin Healey, NIOC Colorado
CTRCS Robert Jacobsen, CSG MacDill AFB
CWO2 Jason Johansen, NIOC Maryland
CTRCS Scott Kelton, NIOC Maryland
CTRC Garrett Kitterman, NIOC Colorado
CTTC Brady Labrum, NIOC Hawaii
CTIC Suellen Leach, NIOC Maryland
CTR1 Wynoka Munlyn, NIOC Maryland
CTRC Anthony Peterkin, NIOC Misawa
CWO3 Donald Robinson, Jr., NIOC Maryland
LCDR Julio Sanchez, SUSLAK Korea
CTI1 Sara Troup, NIOC Texas
CAPT Linnea Sommer-Weddington, US Forces
Afghanistan
CTRC Stanley Thrush, Jr., NIOC Colorado
CTRC Denise Vola, CSG MacDill AFB



MERITORIOUS SERVICE MEDAL

CDR Vincent Augelli, NCTS Guam
CDR James Baca, NR NIOC San Diego
ETCM Timothy Borrer, NAVNETWARCOM
CTMCS Michelle Bradley, FLTCYBERCOM
CDR William Carter, NIOC San Diego
CTTCS Gary Davis, NIOC Georgia
CDR Joel Davis, NIOC Norfolk
CDR Michael Douglas, NIOC Yokosuka
CDR Michael Elliot, NIOC Maryland
ITCM Roderick Florentino, NCTS Bahrain
CDR Thomas Fulford, III, FLTCYBERCOM
LCDR Matthew Ghen, NCTS San Diego
CDR Cheryl Gotzinger, NR NIOC Hawaii
CDR Mark Guzzo, NAVCYBERFOR
CDR Jeffrey Jakuboski, NIOC Colorado
CDR Eric Johnson, NCTAMS PAC
LCDR Timothy Krippendorf, NIOC Georgia
CAPT Ann Litchfield, NR NAVNETWARCOM-SPACE
LCDR Calvin Loper, CMIO Norfolk
CTRCS Jonathan Maddalena, FLTCYBERCOM
CDR Jacqueline McElhannon, NCTAMS LANT
CDR Albert Musselwhite, NIOC Menwith Hill
CDR Jason Parish, NIOC Sugar Grove
CTRCS William Penning, FLTCYBERCOM
LCDR James Reilly, NAVCYBERFOR Colorado
LCDR Andrew Rinchetti, NAVCYBERFOR
CDR Rachel Velasco-Lind, NIOC Maryland
LCDR Joshua Vergow, NIOC Bahrain
CTICM Joseph Wachtler, NIOC Bahrain
CDR Michele Watson, NAVCYBERFOR
CMDMCM Terry Watson, NIOC Hawaii
CMDMCM Donald Wilson, NIOC Norfolk
CDR Daryk Zirkle, NIOC Norfolk



JOINT SERVICE COMMENDATION MEDAL

CTN1 Hyatt Abdelghani, NIOC Maryland
CTR1 Jonathan Ackley, NIOC Hawaii
LTJG Anthony Akil, Kandahar City, Afghanistan

CTT1 Luis Avalos, NIOC Colorado
CTR1 Jason Ayres, NIOC Maryland
CTI2 Gregory Banks, NIOC Texas
CTT2 Patrick Behan, NIOC Colorado
CTI2 Brian Blacher, NIOC Maryland
CTN2 Christopher Bostwick, NIOC Maryland
IT1 Jonathan Bryant, NIOC Maryland
CTR2 Zachary Camburn, NIOC Hawaii
LT Joseph Cantu, Jr., NIOC Maryland
CTR1 Brian Chase, NIOC Maryland
CTR1 Bryan Clack, NIOC Colorado
CTN2 Nicholas Clayton, NIOC Georgia
CTT1 Jeffrey Cormier, NIOC Colorado
IT2 Randi Dean, NIOC Maryland
CTT2 David Dunbar, NIOC Colorado
CTN1 Brandon Desimone, NIOC Maryland
YN1 Harriet Douglas, NIOC Maryland
CTR2 Marriette Edwards, NIOC Maryland
CTR1 Timothy Fairbanks, NIOC Colorado
CTRC Heather Fay, NIOC Maryland
LT Christopher Foster, NIOC Maryland
CTT1 Fredrick Foutz, NIOC Texas
CTR1 Craig Frase, NIOC Maryland
CTI1 Michelle Goodman, NIOC Maryland
LT Nathaniel Grebb, NIOC Maryland
CTT1 Jonathan Green, NIOC Colorado
CTT1 Thomas Greene, NIOC Colorado
CTT1 Benjamin Gresham, NIOC Texas
CTI1 Timothy Gunderson, NIOC Hawaii
LTJG Joseph Hake, NIOC Maryland
CTT2 Todd Harry, NIOC Colorado
CTR2 Jordan Hartke, NIOC Hawaii
LTJG Blake Henderson, NIOC Texas
CTR2 Lauren Hershey, NIOC Hawaii
LT Joseph Hess, NIOC Maryland
IT1 Eugene Hill, NIOC Maryland
LT Leighton Hill, NIOC Maryland
CTI1 Chi Hill-Mann, SUSLA Korea
CTR2 Cory Hogan, NIOC Colorado
CTR1 Marcus Houston, NIOC Georgia
CTR1 Kevin Hubbard, NIOC Maryland
CTR1 Robert Infante, NIOC Colorado
CTN2 Praxedes Irizarry-Rodriguez, NIOC Maryland
CTR1 Ross Jacobsen, NIOC Maryland
CTR1 Brandon Jett, NIOC Colorado
CTT2 Daniel Johnson, NIOC Colorado
IT1 Jesse Johnson, NIOC Georgia
CTI1 Timothy Kerr, NIOC Hawaii
LTJG Erik Knebel, NIOC Maryland
CTR2 Christina Knight, NIOC Maryland
CTI1 Emerson Kraus, NIOC Maryland
CTTC Jared Lampe, NIOC Colorado
CTR2 Dustin Legrand, NIOC Colorado
CTT1 Harry Leonard, NIOC Colorado

CTN2 Alexander Lockman, NIOC Texas
CTR1 Das Manninen, NIOC Colorado
LT Jordan McCaleb, NIOC Maryland
CTTC Edward McCormick, Joint Task Force
CTN2 Russell McElroy, NIOC Texas
CTI1 Benjamin Midkiff, NIOC Georgia
CTR1 Jonathan Minton, NIOC Colorado
LT Luis Montoya, NIOC Texas
CTI1 Jamaar Moore, NIOC Maryland
CTR2 Shomari Moultry, NIOC Colorado
CWO3 Chrystena Myers, NIOC Texas
CTTC Michael Neri, NIOC Maryland
CTT1 Gary Okuna, NIOC Colorado
CTI1 Dareth Pray, NIOC Georgia
CTN1 Samuel Richardson NIOC Maryland
CTR2 Jesus Rocha, NIOC Maryland
CTI2 Joseph Salesky, NIOC Hawaii
CTI2 Aaron Schmidt, NIOC Georgia
CTI2 Rebekah Seeger, NIOC Georgia
CTR1 Nathan Sehi, NIOC Hawaii
CTT1 Harley Simmons, NIOC Texas
CTT1 Jeremy Stewart, NIOC Colorado
CTR1 Benjamin Stipp, USSTRATCOM
CTT1 Lawrence Stonebraker, NIOC Colorado
CTR1 Charles Summers, NIOC Maryland
CTN2 Denton Sweat, NIOC Texas
CTR2 Nickalous Toney, NIOC Hawaii
CTT1 Travis Tucker, NIOC Colorado
CTT1 Davon Tyler, NIOC Maryland
CTN2 Michael Valdez, NIOC Maryland
CTR1 Johnny Wade, III, NIOC Colorado
CTT1 Christopher Watt, NIOC Colorado
CTT1 Christopher Weatherly, NIOC Colorado
CTTC Jonathan Westrum, NIOC Colorado
CTI2 Andrew Woodall, NIOC Georgia
CTR2 Jeffrey Worcester, NIOC Menwith Hill
CTR1 John Yzenbaard, NIOC Maryland



NAVY AND MARINE CORPS COMMENDATION MEDAL

ET1 Roberto Acevedo, NCTS Bahrain
LTJG Jason Amiss NCWDG
LT Kitan Bae, NIOC Bahrain
CTRC Frank Barnard, NIOC Hawaii



IT1 Erick Barnes, NCTS Sicily
ITCS Phillip Bates, NCTAMS LANT
LT Jason Becker, NIOC Whidbey Island
ET1 Jerry Behimino, NCTS FE DET Okinawa
LCDR Adam Bellin, NIOC Sugar Grove
LCDR Jose Berrios, NIOC Yokosuka
ETCS Ryan Biggin, NCTS Naples
ITC Taheshea Birmingham, NCMS Washington DC
ITC Anthony Black, NAVNETWARCOM
CTR1 David Bogan, FLTCYBERCOM
IT1 James Boger, NIOC Colorado
LT Darwin Bowens, NCTS Jacksonville
YN1 Daniel Boyd, NIOC Hawaii
CTI1 Roderick Broach, NIOC Hawaii
CTR1 Brian Britten, NCWDG
LT Michael Brodhead, NIOC Georgia
ITC Danny Brooks, NCDOC
ISC Charles Brown, FLTCYBERCOM
GySgt Christopher Browning, NCMS Washington
ITCM Eric Burch, NCTS Bahrain
CTR1 Bryan Burcham, NCWDG
ITC Anthony Burden, NIOD Groton
CTT1 Brynn Burnash, NIOC Norfolk
ITC John Butler, NAVNETWARCOM
ITC Curtis Buzard, NCDOC
ITCS Dwayne Calhoun, NCTAMS LANT
LCDR Bobby Carmickle, NCTAMS LANT DET HR
LSC Lawrence Carrier, NIOC Sugar Grove
IT1 Kristin Carter, NCTAMS LANT DET Rota
LT Christopher Casey, NAVCYBERFOR
LCDR Miguel Castellanos, NIOC Georgia
LCDR Jessie Castillo, NCTAMS LANT
LT Eren Cataloglu, NIOC San Diego
ETC Howard Chambers, II, NCTS FE DET Diego Garcia
CTIC Ariel Chapman, NIOC Georgia
CWO4 James Clary, NIOC Texas
CTTC Clemeshia Cooper, NIOC Norfolk
IT2 Yolanda Corro, NCDOC
LT Joshua Corney, NIOC Bahrain
LT Benjamin Click, NCWDG
CTR1 Laura Coleman, NIOC Hawaii
LT Taysha Colon, FLTCYBERCOM
LT Patrick Condren, NIOC Yokosuka
LT Peter Crimmins, NIOC Texas
ITC Tiffany Croshaw, NMCI DET Norfolk
ITC Tiffany Curry, NCTAMS PAC
CTTC Larry Daughtery, NIOC Hawaii
CWO3 Felix Dealba, NCWDG
CTR1 Timothy Deaton, NIOC Georgia
CTNCS Rafael Del Valle, Jr., NCDOC
CTRC Adrian Delaney, NCWDG
LS1 Dexter Devonish, NCMS Washington

LCDR Paul Doe, NR NAVCYBERFOR
ITC Allen Drum, Jr., NCTAMS LANT
LTJG Shenequa Dunn, NIOC Bahrain
LCDR David Dwiggin, Jr., NCWDG
CWO2 Jason Eatchel, NIOC Misawa
CTT1 Rena Engelhardt, NAVNETWARCOM
YNC Tracey Flemons, NIOC Texas
LT Geoffrey Flowers, NAVCYBERFOR
CTTC Cassandra Fowler, NIOC Norfolk
ITC William Fraley, NAVNETWARCOM
CWO3 Gwendolyn Frazier, NCWDG
CTICS Kasey Gallardo, NIOC Texas
IT1 Kendall Gaston, NCTS Bahrain
CTRCS William Gaudreau, Jr., NIOC Pensacola
LTJG Donald George, NIOC Hawaii
LT Brendan Geoghegan, NCTS Bahrain
CTTCS Stephen Gilreath, NIOC San Diego
LT Mark Gonyea, NR NIOC San Diego
IT1 Amaris Gonzalez, NAVNETWARCOM
ET1 Travis Gort, NCTAMS LANT
CTRC Andrew Griffiths, NCWDG
CTR1 Zachary Gross, NIOC Hawaii
LT Michelle Guenther, FLTCYBERCOM
LCDR David Gutierrez, NIOC Colorado
OSCS Marlon Hammond, NR NIOC Norfolk
CDR Bobby Hand, Jr., NCTAMS LANT
LT Gregory Hand, NCTAMS LANT
YNCS Lamar Harris, NCTS Guam
CWO3 Camille Harwell, NIOC Norfolk
NCC David Hawkes, NCTAMS PAC
CTI1 Nathan Hebert, NIOC Georgia
ISC Esteban Hernandez, NCF FIAF DET Norfolk
CWO4 Bryan Holland, NIOC Colorado
CTTC Sandra Hizer, NIOC Norfolk
IT1 Lakilla Holt, NCWDG
YN1 Sarah Howell, FLTCYBERCOM
LCDR Mariangel Ibarra, NCWDG
LCDR Saundra Irving, NAVCYBERFOR
CWO4 James Jacobs, NAVCYBERFOR
LTJG Mark Javate, NIOC Hawaii
LCDR Todd Keeling, NIOC Texas
ETCS Kevin Kennedy, NIOC Norfolk
CWO3 Patrick Kilcran, NR NIOC HI-Phoenix
LCDR David Kliemann, NIOC Norfolk
CTRC Marion Knowles, NIOC Texas
CTICM Michael Kraft, NAVCYBERFOR
CTNC Angela Lamirande, FLTCYBERCOM
ITC Michael Laurie, NCTS Jacksonville
LCDR Linda Laws, NCTS San Diego
CDR Matthew Lear, NCTS Jacksonville
CTMC Vincent Ledonne, NIOC Yokosuka
CTNC Melinda Lee, NCDOC
LTJG Olga Levkovich, NIOC Bahrain

YNC Robert Lewis, NIOC Misawa
CTI1 Evan Lyles, NIOC Bahrain
YNC Monica Lyles, NAVNETWARCOM
ET1 Jonathan Mainhart, NCTAMS LANT
CTI1 Amorita Malagon, NIOC Georgia
CTNC Roger Mamika, NIOC Pensacola
CWO3 Gregory Manassa, NIOC Norfolk
CTR1 Andrea Mangone, NIOC Bahrain
CTR1 Ross Markajani, NIOC Bahrain
LT Robert Marnell, NIOC Georgia
ITC Jimmy Martin, NCMS Washington
CTRC Matthew Mason, NIOC Hawaii
CTR1 Josue Matos, Jr., NAVNETWARCOM
IT1 Larry Mayo, NCTS FE DET Chinhai
CTN1 Bitalo McCastle, FLTCYBERCOM
IT1 Joel Melendez, NAVNETWARCOM
IT1 Frank Miller, FLTCYBERCOM
YNCS Okkerse Miller, NCTS Far East
CSC John Miranda, NAVCYBERFOR
ITCS Christopher Monaghan, NCTAMS LANT
CTN2 Julia Mora, NIOC Pensacola
OSC David Mosley, NAVCYBERFOR
ETC Anthony Myrick, NCTS Sicily
ET1 Daniel Niemeyer, NCTS Bahrain
IT1 Adrian Ochipinti, NCTS Naples
LCDR Ryan O'Connell, FLTCYBERCOM
ITCS Anthony Oliver, NCTAMS LANT DET HR
CTRC David Olson, NCWDG
CTNCM Arnel Oribello, NIOC Norfolk
CTN2 Chelsea Overman, NCDOC
ITC Derrick Owens, NCTAMS LANT
ITC Gregory Pearce, NCDOC
MCCS James Perkins, NAVNETWARCOM
LTJG Adam Pettus, NIOC Maryland
CWO3 James Pietrowski, NR NIOC Maryland
ITC Sean Pigford, NCTAMS PAC
LTJG Richard Pinto, NCTS Naples
ETC Courtney Pitts, NCTAMS LANT DET Hampton Roads
CTMC Steven Pope, NIOC Norfolk
CTNC Rita Powell, FLTCYBERCOM
LTJG Peyton Price, NIOC Maryland
IT2 Jonathan Prince, NCTS Naples
ITC Rhonda Randolph, NCTS Bahrain
CTR1CM Geoffrey Reeves, NIOC Maryland
IT1 Nathan Richards, NCDOC
ITCS Teddy Ripley CMS TRNG TM Puget Sound
ITCS Della Roach, NAVCYBERFOR DET San Diego
CWO3 Daniel Robbins, NR NIOC Devens
CTRC William Roberts, NIOC Hawaii
IT1 Carlos Rodriguez, NCTAMS LANT DET Rota Spain
ET1 Danny Roth, NCTS Jacksonville
IT1 Jacob Ruiz, NCTS Bahrain
LT Heath Russert, NCTAMS PAC DET Puget Sound

CTICS Jeffrey Salazar, NAVCYBERFOR
LT William Sandifer, II, NIOC Georgia
CTN1 Terrence Savala, FLTCYBERCOM
ITCS Bradley Schaab, NCTS Bahrain
LT Ryan Shroyer, NIOC Misawa
CTRC Jamel Singleton, NIOC Yokosuka
HMC James Siwert, NIOC Texas
ISC Jeanna Smalligan, FLTCYBERCOM
ITC Christopher Smith, NCTAMS LANT
CDR Mark Smith, NR COMTENTHFLT
CWO4 Mark Spahn, NAVCYBERFOR
LT David Spalding, FLTCYBERCOM
CWO2 Tracy Spivey, NAVNETWARCOM
LCDR Patrick Staub, NAVCYBERFOR
LT Kelly Steele, NAVCYBERFOR
LT Mark Stewart, NCTS Naples
CWO4 Gregory Stone, NAVCYBERFOR
CTN1 Clifford Stout, NCDOC
CTICS Leah Strebin, NIOC Misawa
CTR1CM Todd Strebin, NIOC Hawaii
LCDR Otis Summers, NCTS FE DET Diego Garcia
CTR1 Mathew Takae, NIOC Misawa
LCDR Amir Tavakolirizi, NIOC Georgia
LCDR Seth Taylor, NAVCYBERFOR
LT Robert Terchunian, NIOC Pensacola
LCDR John Tevis, FLTCYBERCOM
IS1 Jamie Thibeault, FLTCYBERCOM
CWO3 Joseph Thomas, NCTAMS PAC
CTRC Wayne Thomason, NCWDG
CWO2 Jimmy Thompson, NCTS Bahrain
CTNC Michael Tonglet, NCDOC
LT Robert Toohig, NAVSOC Point Mugu
CTTCS Von Torres, NIOC Whidbey Island
CTIC Kim-Huong Tran, NIOC Hawaii
LCDR Yolanda Tripp, NCTAMS LANT
YNC Theresa Tucker, NIOC Norfolk
CTRC Jacob Turner, NIOC Hawaii
ITC Danny Vines, NCTAMS PAC
CTN1 Patrick Voight, NCDOC
LCDR Stephen Vossler, NCTS Sicily
CWO2 Michael Wang, NIOC Bahrain
LT Paul Ward, NIOC Bahrain
ETC Matthew Weaver, NCTS Far East
CDR Christopher Weech, NAVCYBERFOR
CTNC Terrance White, NIOC Pensacola
CDR Victor White, NIOC Georgia
LCDR Michael Widmann, NCTAMS LANT
ITC Laronjay Williams, NCTS Bahrain
YN1 Lorena Williams, NIOC Hawaii
CTMC Damon Wirta, NCDWDG
CTNC Robert Wolf, NIOC Pensacola



LTJG Clinton Woods, NIOC Georgia
CTN2 Joshua Wyatt, NCDOD



JOINT SERVICE ACHIEVEMENT MEDAL

CTN3 Rachel Adamick, NIOC Georgia
IT2 Bradley Alspaugh, SUSLA Korea
CTI1 Vanessa Anderson, NIOC Georgia
CTNC Christopher Bareham, NIOC Maryland
CTR3 Donisha BehnBatista, NIOC Hawaii
CTI1 Janka Brock, NIOC Maryland
CTT1 Samantha Bullock, NIOC Colorado
CTR3 Andrew Burns, NIOC Maryland
CTI1 Melissa Caban, NIOC Maryland
CTN2 Jerry Carpenter, NIOC Georgia
CTR2 Stephanie Christensen, NIOC Sugar Grove
CTN3 Richard Clark, CJTF Afghanistan
CTI2 Robert Crawfoot, SUSLA Korea
CTM3 Joel Davis, SUSLA Korea
CTR3 Adam Dempsey, NIOC Maryland
CTI3 Richard Dubbelde, SUSLA Korea
CTT2 Sephra Dyal, NIOC Colorado
CTR3 Christopher Elsmore, NIOC Georgia
CTN3 Thomas Farquharson, NIOC Maryland
CTI1 April Faulkner, NIOC Georgia
CTT2 Benjamin Fennick, NIOC Maryland
CTN2 Zachary Flom, NIOC Hawaii
CTI2 John Furlow, NIOC Maryland
CTR1 Daniel Garrido, NIOC Texas
CTR2 Ismael Gonzalezerbiti, NIOC Hawaii
LT Matthew Gottlieb, NIOC Maryland
CTI1 Chi Hill-Mann, SUSLA Korea
ITSN Christopher Hogan, SUSLA Korea
CTR3 Joseph Jesolva, NIOC Maryland
CTT2 Stephen Johnson, NIOC Colorado
CTT1 Victor Kennedy, NIOC Hawaii
CTR3 Cody Kiser, NIOC Maryland
IT1 Adam Kotschi, NIOC Hawaii
CTR3 Mark Lanouette, NIOC Texas
CTR2 Travis Leonard, NIOC Misawa
CTI2 Destre Mangum, NIOC Maryland
IT2 Marcos Marquez, III, NIOC Hawaii
CTI1 Jesus Martinez, NIOC Hawaii
CTI2 Stephen May, NIOC Hawaii
CTR2 Lauren Maynard, NIOC Hawaii
CTT2 Justin Mays, NIOC Colorado

CTI2 Samantha McGregor, NIOC Maryland
LT Seann McKenna, NIOC Texas
CTT2 Karache Mclin, NIOC Colorado
CTN3 Mario Medina, NIOC Maryland
CTN2 Justin Mercer, NIOC Maryland
CTT12 Nicole Miller, NIOC Texas
CTR2 Timothy Murdoch, NIOC Hawaii
CTI2 Jill Myrand, NIOC Texas
CTR3 Eleya Najarro, NIOC Georgia
CTN2 Jeremiah Nicholson, NIOC Maryland
CTI2 Sean O'leary NIOC Georgia
CTR2 Patrick Ocampo, NIOC Maryland
CTT2 Kyle Overton, NIOC Colorado
CTN2 Matthew Pickich, NIOC Maryland
CTR2 Alexandria Pimentel, NIOC Hawaii
CTI1 Julia Pohl, NIOC Hawaii
CTI2 Timothy Pryor, NIOC Hawaii
CTT2 Christopher Rabjohn, NIOC Colorado
IT1 Gregory Randall, Jr., NIOC Maryland
LTJG Alexandra Reed, NIOC Maryland
CTR1 Eric Reeves, NIOC Georgia
CTO2 Derek Roth, NIOC Texas
CE1 Tito Ruiz, NIOC Hawaii
CTN2 Gary Russell, NIOC Texas
CTR2 Jesse Shreve, NIOC Misawa
CTI1 Angela Sinn, NIOC Hawaii
CTN2 Jarid Smith, NIOC Texas
CTR3 Rea Spencepeterson, NIOC Texas
CTR2 Daniel Stevens, NIOC Colorado
CTT2 Evan Stringer, NIOC Hawaii
CTT2 Abduliszeal Thomas, NIOC Colorado
CTI2 Carlos Thomas, NIOC Hawaii
CTT2 Anthony Toon, NIOC Colorado
CTI2 Michael Towns, NIOC Georgia
CTN2 Cuong Tran, NIOC Maryland
CTN2 Armando Valencia, Jr., NIOC Maryland
CTR2 Caleigh Vazquez, NIOC Hawaii
CTI2 Amanda Vonzirpolo, NIOC Georgia
CTR2 Edward Waltenspiel, NIOC Texas
CTI1 Benjamin Weber, CJTF-HOA
CTI2 Megan Whitt, NIOC Texas
CTR2 Gregory Williams, NIOC Texas
CTI2 J. S. Wilson, NIOC Hawaii



NAVY AND MARINE CORPS ACHIEVEMENT MEDAL

CTR1 Daniel Adkins, NIOC Bahrain
CTN2 Elicha Aguilar, NIOC Pensacola
LTJG Ronnie Alagona, NIOC Hawaii
IT1 Ladedra Alford, NCTAMS LANT NMCI DET Norfolk
IT1 Terrence Alford, NCTAMS PAC DET Puget Sound
CTT2 Christopher Allaman, NIOC Hawaii
IT2 Michael Allen, NCWDG
IT1 Glenn Ames, NCTAMS LANT
IT1 Henry Anders, NCTAMS LANT DET Souda Bay
IT3 Emily Andersen, NCDOD
CTT1 Anthony Anderson, NIOC Georgia
IT2 Jessica Anderson, NCTAMS LANT
IS3 Jarrett Andrewsschiro, NAVCYBERFOR FID Fallon
IT2 Pamela Arvelo-Marrero, NAVCYBERFOR
IT1 Andrew Arz, NCTAMS LANT NMCI DET Norfolk
CTI2 Bryan Ashby, NIOC Hawaii
IT1 Dennis Atkins, NCTS Bahrain
ITCS Steven Ayotte, NCTAMS LANT
CTM1 Benjamin Baird, NIOD Digby
IT1 Brittney Bake, NIOC Norfolk
CTT3 Adolph Baker, NIOC Hawaii
ET3 Jacob Balesi, NCTS Sicily
ETCS Gregory Ballard, NCTAMS PAC DET Puget Sound
ITC Nii Banfro, NCTS Bahrain
IT3 Sabrina Banks, NIOC Norfolk
ISC Stephen Barrow, NCF FID Washington
IT1 Chad Bartow, NCTAMS PAC
LTJG Judith-Hope Bates, NCTAMS LANT
ET3 Timothy Baur, NCTS Bahrain
IT2 Terry Bearb, NCTS Naples
YNC Melanie Beasley, NCTAMS LANT DET Hampton Roads
ET3 Meoshe Beckworth, NCTS Sicily
IT3 Casey Beiter, NCTS Far East
LTJG Camden Bennett, NCF FID Washington
CTN2 Joshua Bert, NCDOD
LS3 Ciara Black, NCTS Naples
IT2 Javier Blake, NCTAMS LANT
CE1 Brian Blodgett, NCTS Sicily
IT2 Jennifer Blower, NCTS Bahrain
IT2 Christopher Bobbitt, NCTAMS LANT
CTN1 James Bodley, NIOC Hawaii
NC1 Michelle Bolden, NIOC Norfolk
CTN1 Jeremiah Bonner, NIOC Norfolk
CTR2 Sierra Booher, NIOC Hawaii
IT3 Kacy Bowman, NCTAMS LANT DET Hampton Roads
CWO2 Kevin Bowser, NIOC Pensacola
CTI2 Boris Brajnikoff, NIOC Georgia
IT1 Thomas Brandt, NCTAMS LANT
IS2 Ryan Breckner, NCF FID Washington
IT1 Tyler Breidenbach, NCTAMS LANT DET Hampton Roads

IT1 Roderick Brice, Jr., NCTAMS LANT
IT2 Melissa Brick, NCTS San Diego
ETC Aaron Britt, NCTAMS LANT
CTR1 Brian Britten, NCWDG
IT2 Warnar Brooks, NCTAMS LANT
IT1 William Brossman, NCTAMS LANT
IT1 Ryan Brough, NCTAMS LANT
IT1 Carl Brown, NCTS Bahrain
IT3 Donald Brown, NIOC Colorado
CTR2 Joseph Brown, NIOC Misawa
CTI2 Meagan Brown, NIOC Texas
IT3 Scot Bruyette, NAVCYBERFOR
IT1 John Bryant, FLTCYBERCOM
CTR2 Benjamin Buehler, NIOC Georgia
IT2 Anthony Burgess, NCTAMS LANT
LTJG Adam Burke, NIOC Maryland
LSSN Nassir Burks, NCTS Sicily
IT3 Kyle Burns, NCTAMS LANT DET Hampton Roads
YNC Ryan Burleson, NIOC Colorado
IT1 Brandon Busby, NCTAMS PAC
CTM2 Bryan Butz, NIOC Hawaii
YN1 Teofilo Cabasada, NCTAMS PAC
CTR2 Mark Callei, NIOC Hawaii
IS1 Robert Campbell, NCF FID Washington DC
IT1 Crystal Campos, NCTAMS LANT DET Hampton Roads
ETC Jena Canell, NCTS Bahrain
IS2 Casey Carper, NCF FID Washington
IT2 Cassandra Carson, NCTAMS LANT
IT1 Arthur Castillo, NCF DET San Diego
ET1 Marion Castle, COMMU DET OKLAHOMA CITY
IT2 Rodger Castro, NCTS Naples
IT3 Adam Cataldi, NCTAMS LANT DET Hampton Roads
CTT2 Jessica Cavanaugh, NIOC Norfolk
LT Jennifer Charlton, NIOC Norfolk
IT2 George Chromy, FLTCYBERCOM
IT2 Katherine Chuckasang, NIOC Norfolk
ETC Kirtus Clanton, NCTS San Diego
IT1 Brett Clark, NCTS Naples
IT1 Mario Clay, NCTAMS LANT NMCI DET Norfolk
IS2 Alicia Cleveland, NCF FID Fallon
IT2 Robert Cleveland, NCTAMS PAC
IT2 Shanika Collins, NCTS Naples
LT Paul Colon, NIOC Norfolk
CTIC Gil Contreras, NIOC Hawaii
IT1 Arrieanne Copeland, NAVCYBERFOR
IT1 Melissa Cothren, NIOC Hawaii
ITC Kevin Cournoyer, NCTS San Diego
ET2 Evan Cramer, COMMU DET Oklahoma City
CTR1 Kevin Crawford, NIOD Jacksonville



CTR1 Christopher Crenshaw, NIOC Hawaii
IT1 Lewis Crisp, Jr., NCTAMS LANT
IT2 Lauren Crosbie, NCTAMS LANT
CTT1 Patrick Cross, NIOC Hawaii
IT2 Narcisco Cruz, Jr., NCDOC
IS2 Victor Cruz, Jr., NAVCYBERFOR FIAF Det Norfolk
LTJG Miguel Cueva, NIOC Hawaii
CTN3 Nicholas Culver, NIOC Maryland
ITSN Martin Curtis, NCTS Sicily
IT2 Shane Curtis, NCTAMS LANT
CTR2 Nolan Dabruzzi, NIOC Hawaii
CTR1 Cody Daigle, NIOD Digby
ITC Jason Dawson, NCTS Sicily
IT1 Jeffrey Deal, NCTAMS LANT DET Rota
IT2 Scott DeFiesta, NCTAMS PAC
CTR2 Jonathan Demarco, NIOC Bahrain
LS2 Amber Denton, NCTS Sicily
YN2 Roger Deshields, NIOC Bahrain
IT1 Joseph Devlin, NCTAMS LANT
LS1 Dexter Devonish, NCMS Washington
IT1 Frederica Donald, NCTAMS LANT
CTRC Jafious Dorsey, NIOC Hawaii
CTR2 Pierre Douglas, NIOC Hawaii
CTRC James Doutt, NIOC Georgia
IS2 Spencer Doyne, NCF FIAF DET Norfolk
CTR2 John Drum, NIOC Yokosuka
IS1 Thierry Duff, NCF FIAF DET Norfolk
IT3 Katie Dugan, NCTS Bahrain
CTR2 Brandon Dunn, NIOC Georgia
CTT1 Matthew Dunsford, NIOC Hawaii
ITC Terry Eady, NCTS Naples
ET2 Mark Eaves, NCTS Naples
IT1 Nicholas Eddy, NAVNETWARCOM
IT3 Ashley Edwards, NIOC Norfolk
CTR1 Kyle Edwards, NCWDG
ITC Jacqueline Elisca, NCTS Bahrain
FC2 Tiyony Ellingson, NIOC Hawaii
IT1 Jonathan Ellison, NCTAMS PAC
ITC Victor Encarnacion, NCTS San Diego
IS2 Daniel Etchberger, NCF FID Washington
ET1 David Evans, NCTS FE DET Diego Garcia
CTR2 Grant Evans, NIOC Georgia
ITC Ward Ewart, COMMU DET Fairfield
CTT2 Jennifer Fairlie, NIOC Hawaii
IC1 Diane Ferrell, NCTS FE DET Diego Garcia
ET1 Ryan Ferrer, NCTS Sicily
IT1 Rafael Figueroa Colon, NCTAMS LANT
NMCI DET Norfolk
IT1 Rhonda Fleming, NCTS FE DET Diego Garcia
CTN2 Rebecca Foss, NCDOC
CTR1 Jonathan Framstad, NCWDG
CTT2 Joshua Frankel, NIOC Hawaii

CTI2 Christopher Franks, NIOC Georgia
YN1 Adriel Frazier, NIOC Hawaii
CTN2 Vanessa Freeman, NCDOC
IS3 Joseph Galeote, NCF FID Fallon
ITC Lateeyah Gammage, NCTAMS LANT
NMCI DET Norfolk
CTN2 Artysia Gaydennapper, NIOC Pensacola
ET3 Robert Gerwitz, NCTS Bahrain
ITC Warren Gilliland, NCTAMS LANT DET
Hampton Roads
YN2 Alexander Gilmore, NR NIOC Hawaii
ITSN Joshua Glaser, NCTS FE DET Singapore
OS1 Kenneth Glasscock, NAVCYBERFOR
LT Tebin Glebus, NIOC Georgia
IT1 Miguel Gomez, NCTS San Diego
CTI1 Donna Gordon, NIOC Texas
ET2 Jermaine Gordon, NCTAMS LANT
CTTC Demetrios Gourgoulanis, NIOC Norfolk
IT2 Nicholos Graves, NCTS Naples
CTN3 Ashley Gray, NIOC Pensacola
IT2 Jermaine Gray, NCTS Bahrain
LT Lisa Green, NIOC San Diego
ET2 Samantha Green, NCTS Bahrain
IS2 Sean Grimes, NCF FID Fallon
CTR2 Joshua Grohoski, NIOC Hawaii
IS2 Todd Guillen, NCF FID Fallon
IT1 Noah Guttsen, NCTAMS LANT
IT1 Andrew Hackett, NIOC Norfolk
CTR1 Charles Hall, III, NIOD Digby
IT1 Robert Hall, NCTAMS LANT
CTI1 Nicholas Ham, NIOC Misawa
IT2 Kivia Hammock, NCTS Jacksonville
IT1 Rocio Hammond, NCTAMS LANT
LT Michael Hanna, NCTAMS PAC
ITC Jeffery Hansen, NCTAMS LANT NMCI DET Norfolk
IS2 Robert Hansen, NCF FIAF DET Naples
CTN3 Nicholas Harlan, NIOC Pensacola
IT2 Jonathan Harris, NCMS Washington DC
YN1 Pier Harris, III, NCTS Bahrain
CTR3 Sean Harris, USS BENFOLD
LTJG Andrew Heil, NIOC Maryland
CTR1 William Hemming, NIOC Georgia
LTJG Joshua Hicks, NAVNETWARCOM
ET3 Cassandra Hipolito, NCTS Jacksonville
ET3 Courtenay Hippert, DET OKLAHOMA CITY
CTR3 Shannon Hobson, NIOC Georgia
LS2 Vincent Hodges, NIOC Norfolk
ET2 Stacie Hoffman, NCTS Far East
IS2 Ryan Holman, NCF FID Fallon
CTI1 Kyle Holmberg, NIOC Georgia
ETC Gregory Holt, NCTAMS LANT
LS2 Mark Homans, NCTAMS LANT DET Rota

IS1 Kelli Homza, NCF FID Washington DC
CTIC Hugh Hooper, III, NIOC Bahrain
IT3 Bradley Hopkins, NCTS Sicily
ITC Richard Hopp, NCTAMS PAC
IT2 Samuel Hopper, NCWDG
IT1 Robert Hortaleza, NAVCYBERFOR DET San Diego
IT1 Demetria Horton, NCTAMS LANT
CTR2 Dana Howard, NIOC Georgia
CTM3 Steven Howard, NCWDG
CTT1 Clifford Howe, NIOD Kaneohe Bay
LTJG Douglas Howell, NIOC Georgia
EM2 Ashley Howley, NCTS Sicily
CTN3 Sergio Hughes, NIOC Texas
IC1 Saul Hurtado, NCTAMS LANT DET Rota Spain
LS1 Noghayin Idele, NAVCYBERFOR
YN1 Jacqueline Irwin, NIOC Hawaii
CTI1 Kirk Iseli, NIOC Misawa
CTT2 Seanna Izzo, NIOC Hawaii
IT2 Brian Jackson, NCTAMS LANT
LTJG Matthew Jackson, NIOC Texas
YN1 Nereida Jackson, NIOC Hawaii
CTR2 Kaden Jacobs, NIOC Georgia
CTR1 Alexander James, NIOC Georgia
ET3 Kyle James, NCTS Sicily
IS3 Michael Jarvis, NCF FIAF Norfolk
CTR1 Alfredo Jauregui, NR NIOC Hawaii
ET3 Audia James, NCTS Jacksonville
IT3 Carmel Jeanmichel, NAVCYBERFOR
IT2 Sean Jenei, NCTS Sicily
CTI2 Christopher Jenkins, NIOC Georgia
IT3 Bianca Jimenez, NCTS Bahrain
IT1 Daniel Jimenez, NCTAMS LANT NMCI DET Norfolk
CTR1 Dorothy Jimenez, NIOC Norfolk
CTT2 Timothy Johlman, NIOD Kaneohe Bay
IT1 Carrie Johnson, NCTAMS PAC
IT2 Jeremy Johnson, NCTS FE DET Atsugi
IS1 Kenny Johnson, NAVCYBERFOR FIAF DET Norfolk
ITC Ulyssa Johnson, NCTAMS LANT DET
Hampton Roads
IT1 George Jones, NCTS FE DET Okinawa
IT1 Hunter Jones, FLTCYBERCOM
CTM1 Vincent Kandian NIOC Norfolk
IT1 Robert Kantrowitz, NCTAMS LANT
IT3 Daunte Kelly, FLTCYBERCOM
IT1 Jarred Kendall, NCTAMS LANT DET Hampton Roads
CTTC Jessica Kerr, NIOC Hawaii
LS2 James Ketterer, NIOC Hawaii
CTT2 Sasha Kildow, NIOC Colorado
CTI2 Meghan King, NIOC Hawaii
MA2 Nicholas Kirkland, NIOC Sugar Grove
IT2 Amanda Kisner, NIOC Norfolk
CTI2 Eric Kocher, NIOC Maryland

CTR1 Adam Koolhof, NR NIOC Hawaii
CTI2 Jonathan Koscianski, NIOC Maryland
IT3 Mitchell Krane, NCTS Bahrain
ET1 Michael Kugler, NCTS San Diego
IS1 Jason Lagoe, NAVCYBERFOR FID Washington
IT1 Valinda Lewis, NCTAMS LANT
IT2 Yongze Liu, NCTAMS LANT NMCI DET Norfolk
IT2 Erin Long, NCTS Bahrain
CTR2 Brittney Lopez, NIOC Hawaii
IT2 Samantha Lopez, NAVNETWARCOM
ET2 Scott Love, NCTS Sicily
IT2 Heather Lustgraaf, NIOC Norfolk
IT3 Kristopher Mackey, NCTS Sicily
IT2 Christal Madison, NCDOC
ET2 Nguyet Mai, NCTS Naples
IT2 Camella Majors, NAVCYBERFOR DET San Diego
IT2 Jasper Mallari, NCTAMS PAC
CTT1 James Mancha, NIOC Georgia
ET2 Stephen Mancini, NCTS Bahrain
CTR1 Das Manninen, NIOC Colorado
ET1 William Mapp, NCTS Guam
YN2 Daniel Marcum, NIOC Yokosuka
IT2 Robert Markley, NCTAMS LANT DET Hampton Roads
IT2 Stuart Marks, NCTS Sicily
ET1 Matthew Martin, NCTAMS LANT DET
Hampton Roads
IT2 Jesus Martinez, NCTAMS LANT
CTI1 Haley Matthews, NIOC Bahrain
IT1 Henry Matthews, Jr., NCTAMS LANT
NMCI DET Norfolk
CTT3 Anika Maynard, NIOC Hawaii
IT2 Latanya Mazyck, NCTAMS LANT
EM3 Stefanie McCann, NCTAMS LANT
IT3 George McCoy, NAVNETWARCOM
ITCS Sheridan McCray, NCTAMS LANT
IT2 Claudia McGuire, NCTAMS LANT
CTM1 Isaiah McHugh, NIOD Groton
IC2 Brad McKay, NCTAMS LANT DET Rota
CTR2 Zachary McKinney, NIOC Hawaii
CTI1 George McLean, NIOD Jacksonville
CTN2 Matthew McNamara, NIOC Pensacola
IS2 Otto McNaughton, NCF FIAF DET Norfolk
ET1 Petra McNutt, NCTS Jacksonville
IS2 Ameer McRae, NCF FID Washington DC
CTI1 Catheryn McShane, NIOC Texas
YN1 Jennefer Meneses, NAVCYBERFOR DET San Diego
IT2 Merced Mercado, NCTS Naples
IT1 Germain Metayer, NCTAMS LANT DET Rota
CTI1 Amy Mikolajczyk, NIOC Georgia
IT1 Brady Miller, NCTS Far East



IT1 Lorenzo Miller, Jr., NCTAMS LANT DET Hampton Roads
ET1 Vaughn Miller, NCTAMS PAC
IT1 Aaron Mitchell, NCTS Naples
IT1 Sydney Moat, NIOC Norfolk
ITC Johnathan Montealegre, NCTAMS LANT DET HR
CTM1 Mary Moore, NIOC San Diego
CTR2 Meagen Moore, NCWDG
IT1 Terrance Moore, NCTS Bahrain
IT2 Andrew Moreno, NCTAMS LANT
CTI1 April Mule, NCWDG
IT1 Erica Mundo, NCTS Sicily
ITC Shawn Myers, NCTAMS LANT DET Hampton Roads
IT1 Rachel Myles, NCTAMS LANT
CTN1 Kuwanda Nathan, NIOC Norfolk
CTI1 Michael Nail, NIOC Bahrain
ET2 Nathan Naylor, USS WHIDBEY ISLAND
LT Jeremy Nerius, NIOC Norfolk
CTT2 Brian Neukom, NIOC Bahrain
CTN1 Andrew Nguyen, NIOC Hawaii
IT2 Joseph Nicks, NCTS Naples
CTT1 Benjamin Northcutt, NIOC Hawaii
IT2 Jason Obleton, NCTAMS PAC
YN1 Jefferson Ocampo, NIOC Hawaii
LCDR Joseph Oconnell, FLTCYBERCOM
ET2 Brandon Opena, NCTAMS PAC
CTM2 Eric Ornelas, NIOC Hawaii
CTN1 Adam Overman, NIOC Norfolk
CTT2 Kevin Owens, NIOC Georgia
IS3 John Parker, NIOC Maryland
QM2 Kortnye Parker, NCTAMS LANT
IT2 Brian Parr, NCTSCU DET Fairfield
LT Robert Parsons, NCTS Bahrain
CTI1 Sarah Pascoe, NIOD Kaneohe Bay
ITC Jennifer Pate, NAVCYBERFOR
IT2 Heidi Patrick, NCTS San Diego
LTJG Isaac Patterson, NIOC Texas
IT1 John Pauley, NCTS Sicily
ET2 Damien Pauline, NCTAMS LANT Norfolk
CTR1 Francisco Peavy, NIOD Jacksonville
CTI1 Alana Pechon, NR NIOC Hawaii
IT2 Digna Pennington, NCTAMS PAC
YN2 Sean Pepler, NIOC Colorado
IT1 Michelle Perry, NCTAMS LANT NMCI DET Norfolk
YN1 Shakina Perry, NCTS San Diego
CTMC Christopher Peterson, NCTAMS PAC
CTI3 Kevin Peterson, NIOC Texas
CTR2 Alec Ploof, NIOC Hawaii
CTR1 Richard Poe, NCWDG
ET2 David Porter, Jr., NCTS Jacksonville
CTR2 Anthony Porterfield, NIOC Hawaii
ET3 Anthony Potter, NCTAMS LANT

CTTC Lewis Proffitt, Jr., NIOC Norfolk
IS1 Nicole Pugh, NIOC Norfolk
CTR1 Nicholas Pujado, NIOC Hawaii
IT2 Kristoffer Quiambao, NCTS Guam
CTN2 Diego Quinones, NIOC Pensacola
IT2 Michell Rabun, NCTAMS LANT DET Hampton Roads
LTJG Brett Rajchel, NIOC Georgia
OS2 Nakita Ray, NCTAMS LANT
IT1 Bernard Rayford, NAVCYBERFOR
CTR2 Holly Rea, NIOC Georgia
CTR3 Kayla Reed, NIOC Hawaii
CTN1 Michelle Reed, NCDOC
IS2 Christopher Rettinger, NIOC Norfolk
ITC Michael Rewerts, NAVNETWARCOM
CTR3 Kedward Reyes, NCWDG
ET1 Jose Reyna, NAVSATCOMFAC Northwest
HM2 Anthony Reynolds, NIOC Hawaii
CTM1 Paul Reynolds, NIOD Groton
IT1 Jeffrey Rhone, NAVNETWARCOM
IT1 Armando Richardson, NCTS Naples
CTR2 Daniel Richardson, NCWDG
IS1 Shawn Richburg, NCF FID Washington DC
IT3 Stuart Ringler, NCTAMS PAC
ITC Daniel Risko, NCTAMS PAC
LT Anthony Rivera, NR NIOC Great Lakes
ITC Richard Rivera, NCTS San Diego
IT1 Tina Rivera, NCTAMS LANT DET Hampton Roads
IT2 Tyler Robertson, NCTS Bahrain
IT2 Jacob Robinson, NIOC Yokosuka
ET3 Tanisha Robinson, NCTAMS LANT DET Hampton Roads
IT2 Charles Robison, NCTAMS LANT
ET2 Joshua Robson, NCTS Bahrain
IT1 Carlos Rodriguez, NCTAMS LANT DET Rota
IT1 Eugene Rodriguez, NCTS San Diego
CTR2 Tomas Gonzalez Rodriguez, NIOC Hawaii
IT2 Desmond Rogers, FLTCYBERCOM
IT1 Juan Roldan, Jr., NCTAMS LANT
CTR2 James Rollins, NIOC Hawaii
IT1 Jean Ross, NCTAMS PAC
CTIC David Roy, Jr., NIOC Georgia
YN1 Rosezetta Russ, NCDOC
IT2 Matthew Russell, NCTS Naples
LT Jessica Ryan, NIOC Georgia
CTI2 Ryan Sammons, NIOC Georgia
CTR2 Toni Sampson, NIOC Hawaii
CTN2 Gustavo Sanchez, NIOC Maryland
ET3 Roland Sanchez, Jr., NCTAMS LANT DET HR
IT1 Kandi Sannicolas, NCTS Jacksonville
CTM1 Eric Santorelli, FLTCYBERCOM
IT1 Anthony Scaffidi, NCTS FE DET Chinhae

CWO2 Scott Schwab, NCTAMS LANT Norfolk
CTN1 Dean Schyvincht, NIOC Hawaii
IT1 Kevin Seguin, NCTAMS PAC
CTN2 Danny Sellers, NIOC Pensacola
IS3 Eileen Sempa, NCF FIAF DET Naples
IT2 Larronica Shannon, NCTS Bahrain
LT Peter Sharrai, NAVNETWARCOM
IT1 Adam Shearin, NCTAMS LANT
CTN2 Chance Sheffield, NIOC Pensacola
MC1 Leeanna Shippis, NCWDG
IT1 Larry Showers, Jr., NCTAMS LANT DET Hampton Roads
ET1 Adam Sidun, COMMMU DET PAX River
IT1 Meranda Simmons, NAVNETWARCOM
LT Joseph Simon, NCTS San Diego
IT1 Christopher Simons, NCTAMS PAC
IT1 Edward Sitko, Jr., NCTAMS LANT
IT3 Kayse Slaughter, NCTAMS LANT DET Hampton Roads
CTT1 Geoffrey Small, NIOC Hawaii
ITC Kenya Smarr-White NCTAMS PAC
IT2 Ebony Smith, NCTAMS LANT NMCI DET Norfolk
CTR1 Douglas Smith, NCWDG
CTR1 Joshua Smith, NIOC Georgia
CTR2 Hayward Smith, NIOC Pensacola
CTR1 Samuel Solis, NIOC Georgia
ET2 Adam Soper, NCTAMSLANT DET Hampton Roads
IT1 Justin Soppe, NIOD Digby
IT1 Ian Sorensen, NIOD Digby
ITS1 Omar Sotelo, NCTSCU DET Fairfield
IT2 Christopher Sowards, NCTAMS PAC
MA1 Dana Spalding, NR NIOC Hawaii
LT David Spalding, FLTCYBERCOM
IC2 Steven Spears, Jr., NCTS Naples
CTT1 Jennifer St. Louis, NIOC Norfolk
IT1 Shaun Stanley, NCTS Sicily
CTRC David Steed, NIOC Texas
IT1 Pamela Stephens, FLTCYBERCOM
IT2 Michael Stevenson, NCTAMS LANT
IT2 Cullen Still, NCTAMS PAC
IT3 Megan Stillely, NCTAMS LANT
CTT2 Jesse Stocking, NIOC Georgia
LTJG Joshua Stonehouse, NIOC Texas
CTN1 Clifford Stout, NCDOC
CTR1 Thomas Stout, NCWDG
IT1 Parrish Strong, NCTAMS LANT
CTR3 Rickey Stuckey, NIOC Pensacola
YN3 Iesha Stull, NCTAMS LANT
IT2 James Stuursma, NCDOC
CTT1 Diane Sunday, NIOC Hawaii
CTR2 Arlene Surun, NIOC Hawaii
ITC Christopher Swallow, NCTAMS LANT

NMCI DET Norfolk
CTI2 Samuel Swymer, NIOC Maryland
CTR2 Ryan Tarver, NIOC Yokosuka
IT1 Clint Tayag, NCTAMS PAC DET Puget Sound
CTI2 Kathryn Taylor, NIOD Kaneohe Bay
IT2 William Taylor, NCTAMS LANT
IT1 Bobby Thayer, SPAWARSYSCENPAC
IS2 Michael Thielen, NCF FID Fallon
YN2 Terry Thomas, NCTS Sicily
CTM2 Tanesha Thompson, NIOC Norfolk
IT2 Yaemin Tilley, NCTAMS LANT
CTTC Carolyn Toney, NIOC Norfolk
IS3 Andrea Tourville, NAVCYBERFOR FID Fallon
IT1 Sakita Trammel, NCTAMS LANT NMCI DET Norfolk
IT2 Gabriel Trujillo, NCTS Naples
IT1 Carol Tsung, NCTAMS LANT
CTNC Kevin Tullios, NIOC Maryland
IT2 Austin Tushaus, NCDOC
CTR1 Jessica Ulett, NIOC Yokosuka
LS2 Jose Unciano, NCTS Bahrain
CTIC David Ure, NIOC Bahrain
YN1 Daniel Vasquez, NAVCYBERFOR
CTI1 Ashley Veeck, NIOC Bahrain
CTI3 Daniel Villa, NIOC Texas
IS2 Joshua Waldrop, NCF FID Fallon
CTM3 Cole Walker, NIOC Hawaii
IT2 Terrell Walker, NIOC Hawaii
ET2 Ricky Wallen, NCTAMS LANT
IT3 Dustin Ward, NCTSCU DET Fairfield
LTJG Zachary Wasserman, NCF FID Washington
IT1 William Watton, NCTAMS PAC
CTR2 Samuel Webb, NIOC Hawaii
CTR2 Adam Wehman, NIOC Menwith Hill
CTT2 Donald Wendt, NIOC Georgia
CTI1 Kathryn Werner, NIOC Texas
CTT1 Max West, NIOC Hawaii
IT1 Carl White, NCTAMS PAC
IT3 Christopher White, NIOC Norfolk
IT1 Jeremy White, NAVNETWARCOM
IT2 Keith Whittington, NCTAMS LANT DET Hampton Roads
IT2 Cicely Wiggins, NIOD Kaneohe Bay
CTN2 Charliea Williams, NIOC Norfolk
CTRC Jill Williams, NIOC Norfolk
IS2 Ashley Wilson, NIOC Norfolk
ENS Desmond Wilson, NCTS Far East
IS2 Jeremy Wilson, NCF FIAF Mayport
IT1 Mignone Wolf, NCTAMS LANT DET Hampton Roads
CTR1 Daniel Womack, NIOC Yokosuka
ITC Milena Wood, NCTS Naples



MERITORIOUS CIVILIAN SERVICE AWARD

Tracy Davis, FLTCYBERCOM
 David Philips, NCTAMS LANT
 Jacqueline Rayford, NCTAMS LANT
 Curtis Smith, NCTAMS LANT
 Robert Swafford, NCTAMS LANT DET Hampton Roads
 Martin Tengowski, NCTAMS LANT

CIVILIAN LENGTH OF SERVICE AWARDS

Louis Noah, NCTAMS LANT - 40 Years
 Vaughn Vance, FLTCYBERCOM - 35 Years
 Judy Bareilles, FLTCYBERCOM - 34 Years
 Donna Lacy, FLTCYBERCOM - 30 Years
 Brenda Perry, NCTAMS LANT - 30 Years
 Terry Rogers, NCTS Jacksonville - 30 Years
 Twyla King, FLTCYBERCOM - 25 Years
 Harry Keith, FLTCYBERCOM - 20 Years
 Robernetta Turner, NCTAMS LANT - 20 Years
 Howell Carter, FLTCYBERCOM - 15 Years

Philip Cultera, NCTAMS LANT DET Cutler - 15 Years
 Raymond Biasi, NAVCYBERFOR - 10 Years
 Jorge Castro, FLTCYBERCOM - 10 Years
 Ebony Jarrett, FLTCYBERCOM - 10 Years
 Mia Lee, NCTAMS LANT DET Hampton Roads - 10 Years
 Laura Quezada, NCTAMS LANT DET Hampton Roads - 10 Years
 Charlene Plaine, FLTCYBERCOM - 10 Years
 Suchart Waiyanet, NCTAMS LANT - 10 Years

CTT2 Adam Wright, NIOC Bahrain
 CTR2 Grady Wright, NCWDG
 CTR1 Matthew Wykoff, NR NIOC HI-Phoenix
 IT2 Ryan Yeatts, NIOC Colorado
 CTR2 Jason Yingling, NCWDG
 IT1 Rene Yosinao, NCTS San Diego
 IS2 Adam Young, NCF FIAF DET Naples
 LCDR Andrew Young, FLTCYBERCOM
 IS3 Jared Young, NAVCYBERFOR FIAF Det Norfolk
 IT1 Michael Young, NAVCYBERFOR DET San Diego
 CTI2 Robert Young, III, NIOC Bahrain
 CTI1 Jason Zimmerman, NIOC Bahrain
 IS1 Thomas Zimny, NCF FID Washington DC
 LCDR Lisa Zumbrunn, NIOC Georgia



SUPERIOR CIVILIAN SERVICE AWARD

Eric Markland, FLTCYBERCOM
 James Protin, FLTCYBERCOM



MILITARY OUTSTANDING VOLUNTEER SERVICE MEDAL

IT1 Arthur Castillo, NAVCYBERFOR DET San Diego
 LT John Doyle, NAVCYBERFOR
 LT Leighton Hill, NIOC Maryland
 LS1 Noghayin Idele, NAVCYBERFOR
 CWO3 Derek Jefferson, NCTAMS LANT
 ETC Aaron McCoy, NCTAMS LANT
 CTN2 Matthew McNamara, NIOC Pensacola
 CTT1 Jared Miyashiro, NCTAMS LANT
 CTR1 Wynoka Munlyn, NIOC Maryland
 CTC Matthew Saxton, NIOC Colorado
 CTC Justin Tropp, NIOC Colorado



NCDOC Holds Change of Command

VIRGINIA BEACH, VA – CAPT Douglas A. Powers (right) relieved CAPT Alan F. Kukulies (far right with RDML Herbert) as Commanding Officer of Navy Cyber Defense Operations Command (NCDOC) during a change of command ceremony at the Gator Theater on Joint Expeditionary Base Little Creek Fort Story, Aug. 9.



Photos by Michael J. Morris, NETWARCOM Public Affairs

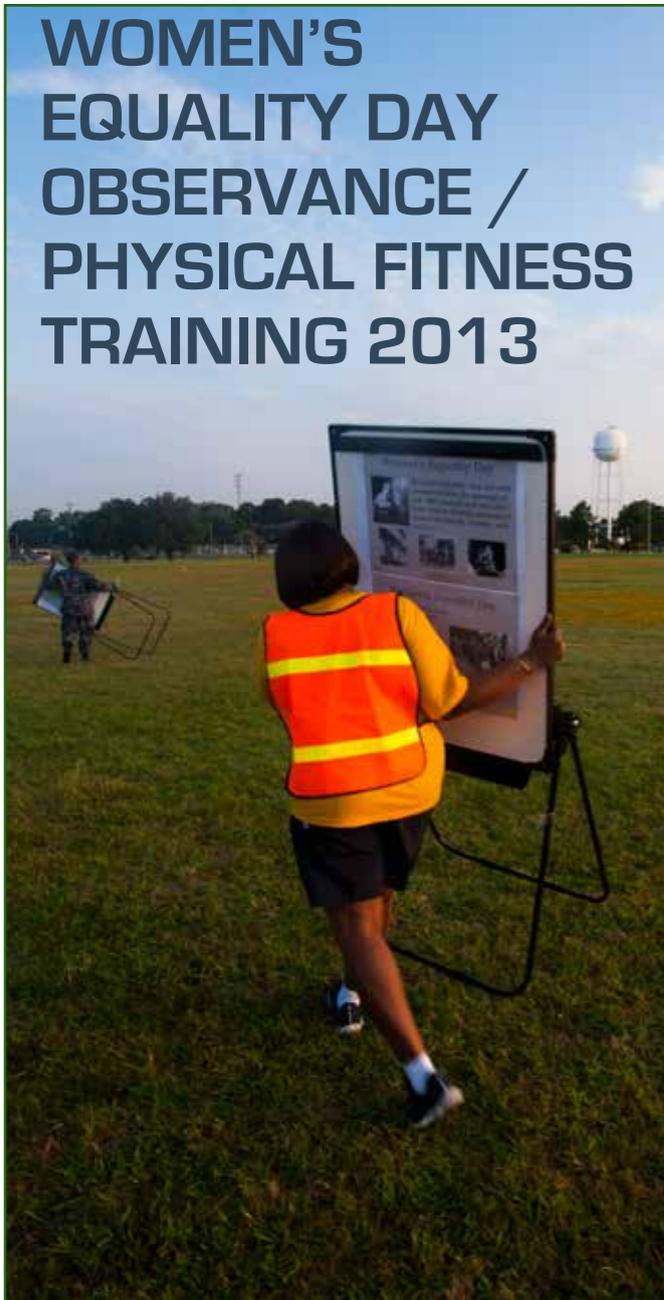




NAVCYBERFOR personnel at JEBCFS got together early on Aug. 22, to commemorate and celebrate the passage of the 19th Amendment to the Constitution that granted women the right to vote.



InfoDIVERSITY



**WOMEN'S
EQUALITY DAY
OBSERVANCE /
PHYSICAL FITNESS
TRAINING 2013**



NAVCYBERFOR Chief Of Staff, CAPT Bennie Sanchez, kicked off the combo commemoration/physical training event reflecting on serving early in his career, aboard a ship with an attached Carrier On board Delivery (COD) squadron that had three women as part of their staff.

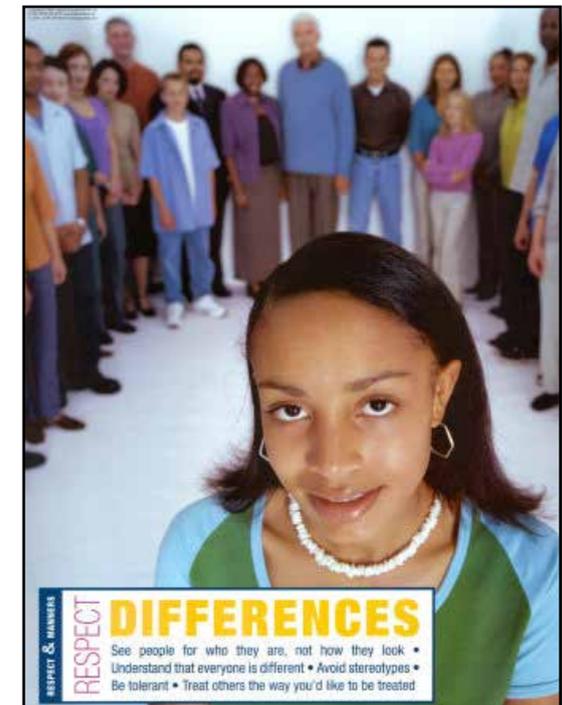
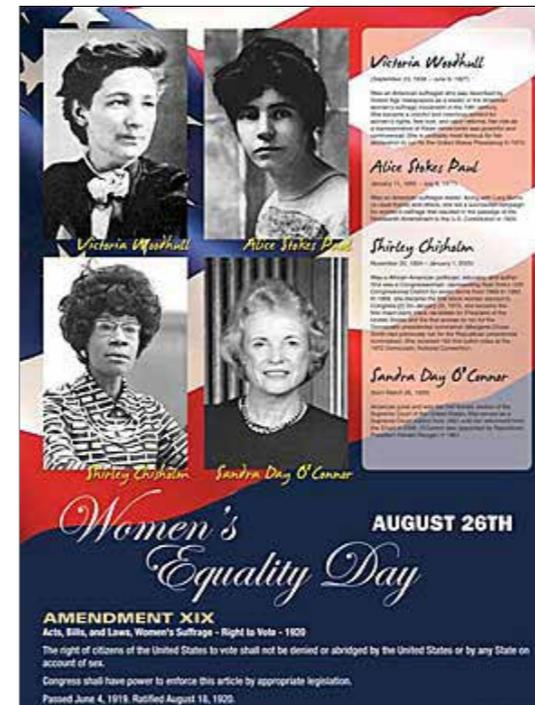
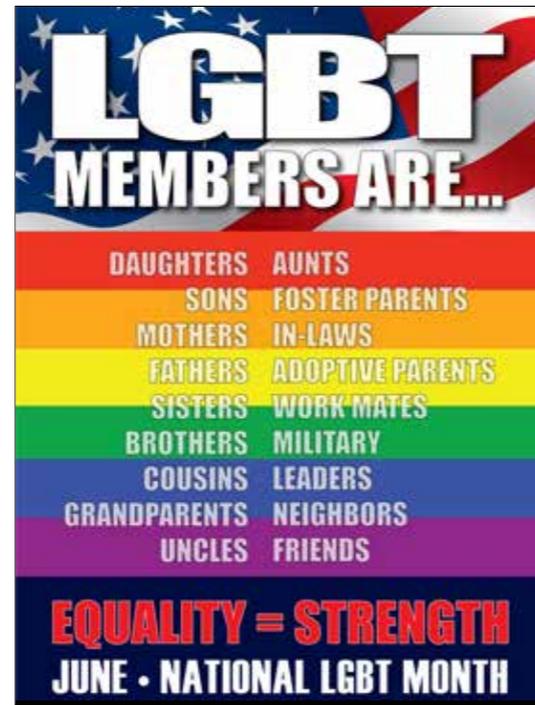
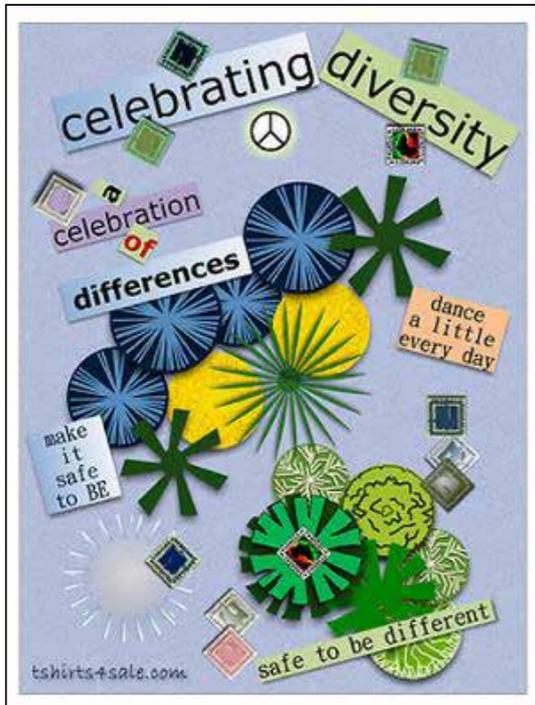




Susan Lowry (right), MWR fitness instructor, leads more than 50 military and civilian participants in warm-up exercises. Fourteen exercise stations were established with informational billboards strategically placed between stations prompting participants to stop and read and remember. ITCS Lisa Dillard and CTN1 Amber Moore spearheaded the event.



Photos by Jacky Fisher & Robin Hicks



LOOK FOR US ON THE WEB

www.cyberfor.navy.mil

or

www.facebook.com/USNavyCyberForces



Summer Edition