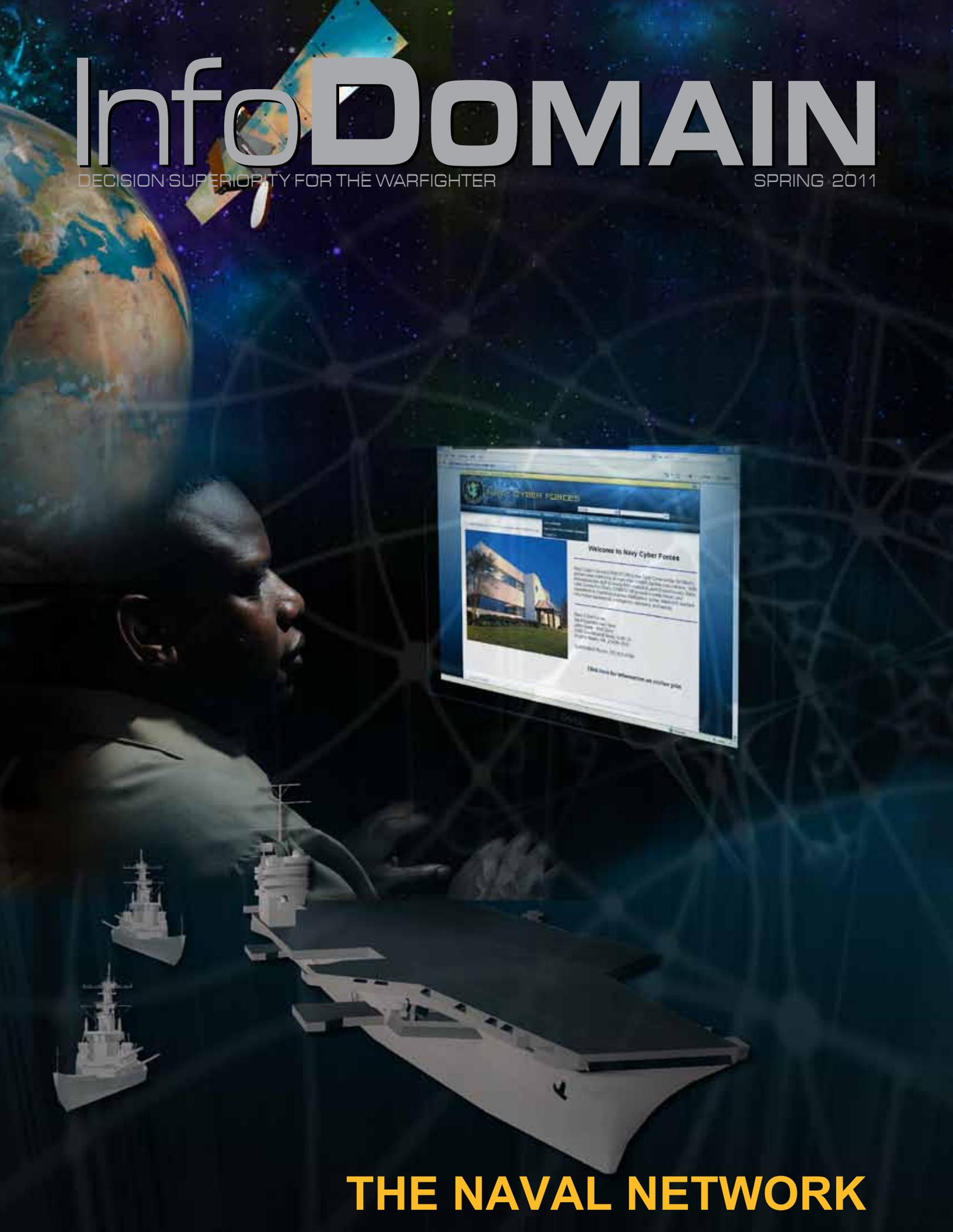


InfoDOMAIN

DECISION SUPERIORITY FOR THE WARFIGHTER

SPRING 2011



THE NAVAL NETWORK



Commander, Navy Cyber Forces
RADM Tom Meek

Deputy Commander
Mr. F. Scott DiLisio

Public Affairs Officer
Ms. Darlene Goodwin

Deputy PAO / Editor
Mr. George D. Bieber

Associate Editor
MC2(SW) Joshua J. Wahl

Visual Information Specialist
Mr. Robin D. Hicks

Production
Quintessential Color Group
Upper Marlboro, MD

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, *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

VADM David J. "Jack" Dorsett
Deputy Chief of Naval Operations
for Information Dominance (N2/N6)
(Official U.S. Navy Photo)



FEATURES

- 3 My Domain**
VADM Dorsett, Deputy CNO ID (N2/N6) reflects on his first year
- 17 Safari Books Online**
MWR funds allow military, retirees & eligible family members usage
- 18 Copernicus Awardees**
NIOC Whidbey Island Sailor and NCDCC employee chosen for award
- 20 AFCEA WEST 2011**
Guest speakers embrace technology & cyberspace
- 22 Corona Warfare Center Wins Top Navy Award**
Center's patented system saves Navy \$65 million
- 23 Navy COOL Wins at 2011 HCMD Awards**
Human Capital Management Defense validates Navy COOL program
- 26 IT Infrastructure Library**
Information Dominance requires superior IT service management
- 28 Virtual Desktop**
Environment helps transform training at FITC San Diego
- 33 Team SPAWAR's CANES Program Meets Goals**
Navy's NGEN tactical afloat network to be introduced in 2012
- 34 IO Range Provides Key Internet Service & More**
Joint IO Range creates flexible, seamless and persistent environments
- 36 Public Key Infrastructure Eases SIPRNet Access**
New PKI certificates on CAC increase ease and security for accounts
- 37 OPSEC Team Reaches Out to Community**
Team provides support during Month of the Military Child
- 42 NIOC Misawa Sailors Aid Japan**
NIOC & NAF Misawa Sailors join forces to aid surrounding communities

DEPARTMENTS

- 5 Force Chaplain's Thoughts**
- 6 CYBERFOR News**
- 10 Short Circuits**
- 12 Letters from the Sea**
- 15 Cyber Warriors**
- 24 CID Spotlight**
- 30 NGEN FITT Update**
- 38 Team Spotlight**
- 44 Special Recognition**
- 48 Diversity**

FRONT COVER: *The Naval Network requires superior IT service management and the IT Infrastructure Library delivers. For more information about the IT Library see pages 26-27. (Graphic Illustration by Robin D. Hicks)*

Information Domain in the Navy – One Year Later

Just over a year ago, we embarked on a transformational effort to reshape the Navy. Our mission is to transform the Navy from a platform-centric institution to one that is information-centric. We are elevating information as a main battery of our warfighting capabilities. Just as carrier aviation in the Second World War and nuclear power in the Cold War gave our nation a strategic competitive advantage, I believe the Navy's information capabilities will deliver a dominant strategic advantage to our nation in the 21st century.

Undertaking such a dramatic transformation required us to take some bold steps, accelerating our investment and deepening our commitment to core information capabilities, particularly in the areas of Electronic Warfare (EW), Cyber, Intelligence, Surveillance and Reconnaissance (ISR), and unmanned systems.

Our People: The Information Dominance Corps

To fully transform the Navy's information capabilities, we are taking an equally aggressive approach to strengthening the capabilities of our information-centric workforce.

CNO created the Information Dominance Corps (IDC) in late 2009 to enable us to take a more comprehensive and integrated approach to the management and development of those members of the Navy Total Force (active, reserve

and civilians) with the information-based skillsets and knowledge needed to provide the warfighting capabilities the Navy needs. We established the Information Dominance Warfare (IDW) program -- with a rigorous IDW Personnel Qualification Standard(s) exams and qualifications for all IDC officers and enlisted personnel, regardless of specific designator or rating.

Professionalization of our information workforce is extremely important. High standards, rigorously adhered to, send a strong message -- not just within the IDC but across the Navy and Department of Defense. Our message is simple: We take our profession seriously and we demand the highest level of proficiency of its practitioners.

In September 2010, we held our first IDC Command/Executive Officer (XO) screening board, modeled after unrestricted line boards and following protocols established by the Bureau of Naval Personnel. In October, IDC leaders developed the detailing slate for FY11 Command/XO/Milestone assignments. We are expanding cross-detailing assignment opportunities to further strengthen our IDC capabilities and Corps identity. And we are maximizing educational programs through new and expanded cyber curriculums at the U.S. Naval Academy, Naval Postgraduate School, and

our traditional accession schoolhouses for officers and Sailors.

Specifically, we are investing in professional development through two milestone career initiatives; the IDC Mid-Career Course at the Center for Naval Intelligence, and the IDC Senior Leadership Symposium at Navy Postgraduate School. The IDC Mid-Career Course is designed to prepare active and reserve 18XX LCDRs for their next tours in the IDC. The IDC Senior Leaders Symposium is designed for 18XX CAPTs, IDC Master Chiefs, and senior civilians (GS15) to focus our leaders on the core competencies of the Corps, including Space, Command, Control, Communications, Computers and Intelligence and Acquisition. These milestones, part of the IDC Training Continuum, are designed to boost our high potential leadership in professional knowledge, skills and abilities through intense intercommunity forums.

In addition, we are partnering with other Intelligence Community members to develop deep penetration solutions to Navy's highest priority intelligence issues. IDC members advocate for Navy equities in numerous Intelligence Community committees, panels and

boards with representation at all levels, from Director of National Intelligence-chaired forums, to working level sessions on specific functional and regional issues. We've also developed close personal

VADM David J. "Jack" Dorsett Deputy Chief of Naval Operations for Information Dominance (N2/N6)

relationships with national Intelligence managers and national Intelligence offices to ensure community production and involvement on Navy interest items.

While we are making great progress in providing a fully qualified force to the Navy, we do not yet possess sufficient depth of expertise in one critical area -- cyber warfare. Therefore we have created two new career paths, Cyber Engineers (1840) and Cyber Warrant Officers, to better leverage both the seasoned experience in our senior enlisted work force and the cutting edge expertise being developed at top-flight universities across the country.

Our Information Dominance Capabilities

In the past year, we have tackled a comprehensive range of capability initiatives, designed to reshape the Navy's warfighting capabilities for the information age. We completed source selection for the Small Tactical Unmanned Air System (STUAS), prepared the Firescout Vertical take-off and unmanned air vehicle (VTUAV) for first deployment, and continued to operate our Broad Area Maritime Surveillance (BAMS) system demonstrator in support of combat operations in the U.S. Central

at a **GLANCE**

VADM David J. "Jack" Dorsett graduated from Jacksonville University (Florida) in 1978. His sea duty included assignments on HMS Gavinton (M1140), USS Elliott (DD 967), USS Oldendorf (DD-972), USS Dominant (MSO-431), USS Ranger (CV 61), deputy assistant chief of staff for Intelligence for commander 6th Fleet, and assistant chief of staff for Intelligence for commander, U.S. Naval Forces Central Command / Fifth Fleet.

His shore assignments included duty at Fleet Ocean Surveillance Information Center commander in chief, U.S. Naval Forces, Europe, U.S. Naval War College, chief of Naval Operations (CNO) Intelligence Plot, the Office of Naval Intelligence, and command of the Joint Intelligence Center, U.S. Central Command.

As a flag officer, Dorsett has served as director of Intelligence (J2), U.S. Pacific Command; director for Intelligence (J2), U.S. Joint Staff; and Director of Naval Intelligence (N2), CNO.

In November 2009, he assumed office as the first Deputy Chief of Naval Operations for Information Dominance (N2/N6).



FORCE CHAPLAIN'S THOUGHTS

In various locations throughout the domain, spring brings many changes with it. Colors turn from brown, gray and white to green, yellow, red or purple. This change in colors is a sign that life is about to change. For some varieties of life, it is the beginning of a new cycle. Something that was dead comes back to life. For others, it is a new birth from a seed that was sown months before. All this activity in nature can and should give humans an opportunity for pause.

Most faith traditions contain concepts of things becoming new at some point in time. A conversion begins a new cycle in the life of the individual. The old person dies out and a new person emerges. For some, change is a constant process as people strive to become more useful tools in the hands of God. The more godliness or 'God-like-ness' attained by the individual, the more useful to God they become.

Change is a constant goal. Improvement always has room to spare. In these faith traditions, change springs forth from a hope in eternity. A seed that was sown corruptible comes forth incorruptible. Something mortal becomes immortal.

As you experience spring, I encourage you to reflect on the newness in nature and evaluate your life. If there is some area that needs renewal or change, take the proper action to create the difference. The Christian tradition uses a nautical picture in its discussion of eternity and hope. It says, "We have this hope as an anchor for our life, firm and secure." I hope that you have a firm and secure anchor for your soul this spring.

Grace and Peace

Chaplain Mac

... continued on Page 6

My Domain continued . . .

Command area of responsibility. In 2010, the BAMS-D flew 113 sorties, with more than 2,043 hours logged, providing high-quality maritime ISR products to decision makers in near real-time. We're also pursuing joint BAMS / Global Hawk initiatives with the Air Force. Our Medium Range Maritime UAS (MRMUAS) program, now working through the acquisition/requirements process, will provide a system that can operate from all air capable ships with flight decks and hangars. It will possess multi-Intelligence collection capabilities, strike capability, and support both line of sight and beyond line of sight mission operations and data reach-back. Our Unmanned Combat Air System Demonstration (UCAS-D) aircraft completed its first flight at Edwards Air Force Base, CA, in early February, paving the way for aircraft carrier flight tests in 2013.

To propel us into the unmanned future beneath the waves, Navy is developing Large Displacement Unmanned Underwater Vehicles (LDUUVs) with the capability to autonomously deploy and manage a variety of sensors and payloads. The Office of Naval Research is leading efforts and working with industry to achieve the power and energy density necessary to extend LDUUV endurance. Our goal is to conduct a fully independent UUV mission by 2017 and to establish an LDUUV squadron by 2020.

We are addressing our future network needs, both afloat and ashore, through the Consolidated Afloat Networks and Enterprise Services (CANES) and Next Generation Enterprise Networks (NGEN) programs. Through NGEN, we are restoring operational control over our networks, while CANES will deliver a streamlined, open architecture for our afloat networks.

As we are revitalizing our traditional EW capabilities through the NGEN Jammer and Surface EW Improvement Program, we are also developing the next-generation of Joint Counter Radio Controlled Improvised Explosive

Device EW (JCREW) to counter threats to the joint force in Iraq and Afghanistan.

Through Task Force Climate Change, Navy has become the recognized global leader in Knowledge of the Ocean Environment. Guided by our Arctic and Climate Change Roadmaps, we are leaning forward to anticipate how we will operate in a future blue water Arctic environment, and we are continuing our transition from hard copy to digital/electronic navigation aids.

We are also fully embracing the Secretary of Defense's guidance to achieve efficiencies across our programs -- not only as responsible stewards of the taxpayers' dollars, but also to give us the flexibility to reinvest savings in our highest priorities. Efficiencies in Information Technology (IT) will be a big part of that, as we pursue thin client initiatives, data center consolidation, voice and video over Internet Protocol (IP), enterprise software licensing and other IT efficiency initiatives within our enterprise IT management effort. We will also seek ways to expand our emerging partnership with the U. S. Air Force, not only in unmanned systems, but also in building the processing, exploitation and dissemination capabilities we will require to handle the explosion in data that has already begun.

I could expand in both scope and depth, but I think you get the message. There is a lot we need to accomplish. It will take the dedicated efforts of each and every one of you in the IDC to maintain and even accelerate the momentum we've already established, and deliver a dominant strategic advantage to the Navy and our nation. I believe we are up to the challenges ahead, and I am more than confident in your abilities to get the job done above and beyond all expectations. I thank you for your continued dedicated service, and look forward to working with you all to tackle the challenges ahead. ✕

Meek Observes DGSIT Program Aboard USS George H.W. Bush

From CYBERFOR Public Affairs

As the Navy's global Type Commander (TYCOM) for Command, Control, Communications and Computers, Combat Systems Interoperability, Cryptology/Signals Intelligence, Computer Network Operations, Electronic Warfare, Information Operations, Intelligence, Networks, and Space, Navy Cyber Forces (CYBERFOR) considers Fleet C5I readiness as its primary deliverable.

One key element in ensuring the Fleet's modernized C5I equipment performance is properly assessed, fully integrated and ready for missions around the globe is the Deploying Group Systems Integration Testing (DGSIT) Program.

Launched well over a decade ago, DGSIT provides this capability through a series of tests designed to demonstrate the ability of newly fielded, installed or upgraded C5I

systems to operate cooperatively in a stressed at-sea operational environment. The DGSIT process considers a Deploying Group's interfacing sensors, applications and networks as a single C5I system, designed to function cooperatively, as an extension of the Naval and Joint Force networks. It also determines how well combat systems sensors collect, process, disseminate and retrieve information

and data in collaboration with other combat systems, through extensive Tactical Data Link test events in all possible architectures and data paths.

In February, CYBERFOR Commander RADM Tom Meek embarked USS GEORGE H.W. BUSH (CVN 77) to evaluate the Final Integration Test (FIT) phase of DGSIT, as the ship participated in a Composite Training Unit Exercise (COMPTUEX) off the Florida coast.

The focal point of Meek's evaluation was to observe the efforts of the DGSIT team as they partnered with the Carrier Strike Group (CSG) units, staff and selected Independent Deployers' executing an extensive test plan tailored to the hardware and software deployment configuration for the GHWB Strike Group.

While embarked, Meek visited the Carrier Intelligence Center (CVIC), Network monitoring and control spaces, numerous radar and sensor rooms, external communications hubs and key combat

direction/command and control spaces. He monitored the extensive interoperability and integration testing conducted by engineers and technicians and coordinated by CYBERFOR's DGSIT team. From Satellite Communications to Digital Air Control and Tactical Data Link live test events, Meek met with subject matter experts and observed them testing and integrating systems as they provided mentoring to shipboard operators and technicians.

"The complex world of C5I requires systems to be complementary and integrated to meet mission," Meek said. "DGSIT provides a comprehensive final review with all of the elements in place: Sailors, staffs, equipment ... all in a pressurized environment to reveal interoperability seams."

According to CYBERFOR's Command and Control Network Operations Division Head, CAPT Kathy Donovan, the goal of DGSIT is to increase confidence among DG commanders in their C5I system operations.

"The DGSIT at-sea team works to identify system limitations and coordinate resolution of issues as they are encountered, and can provide work-around solutions on issues that cannot be immediately resolved," Donovan said.

"Ultimately, this is not an

inspection, but a validation of modernization efforts. Further, it is a unique opportunity to have program office and regional maintenance experts aboard to team with operators and technicians -- to test C5I systems, observe issues, assist in corrections, and to provide operator and technician mentoring on systems under test."

DGSIT Program Director, LCDR Jim McCartney, said another key aspect of the DGSIT process is the value it brings to modernization efforts made by respective program offices.

"Beyond our interaction with the Strike Group and Amphibious Ready Group Commanders, our process also provides formal and actionable feedback into C5I system development, installation, training and life cycle support structure," McCartney said. "Maximum issues which affect mission capabilities result from testing systems in a tactical environment. This aids future development and upgrades to C5I systems."

Meek expects a strong, sustained Fleet demand signal for DGSIT well into the future.

"Given the growing complexity and required C5I integration, we need DGSITs to optimize Fleet C5I capabilities and readiness," Meek concluded. "The return on investment is evident when seen firsthand." ✕

Official U.S. Navy Photo



CYBERFOR, NETWARCOM Celebrate NAVRES Birthday

By Darlene Goodwin, CYBERFOR Public Affairs Officer

VIRGINIA BEACH, VA – Sailors and civilian staff members from Navy Cyber Forces (CYBERFOR) and Naval Network Warfare Command (NETWARCOM) participated in a ceremony commemorating the 96th birthday of the Navy Reserve, at the commands' headquarters on board Joint Expeditionary Base Little Creek, Mar. 3.

CYBERFOR Reserve Affairs Director CAPT Clayton Kemmerer opened the ceremony, acknowledging Navy Reserve members in attendance and reading a birthday message from Chief of Naval Operations ADM Gary Roughead.

Quoting Roughead, Kemmerer said of Navy Reservists, "Your flexibility and responsiveness clearly enhances our Navy as a Global Force for Good. Your selfless dedication and contributions provide strategic flexibility and operational capabilities integral to our forces from homeland defense to our operations forward."

Kemmerer elaborated on the unique and enduring collaborative relationship between the Navy's active and Reserve forces.

"I have often heard senior officers remark about how seamlessly and indistinguishably active, Reserve and (National) Guard personnel blend together," Kemmerer said. "That blended workforce is what we really mean when we say 'Total Force.' Today, as a Total Force, we celebrate yet another birthday in the history of the modern Navy Reserve – a history that, in truth, extends back far more than 96 years – even predating the Continental Navy."

Guest speaker for the ceremony was CYBERFOR



(Above, left to right) YN2 Kassiana Earp, Flag writer for NETWARCOM's commander and CAPT Doug Swanson, assistant COS for Network Operations, NETWARCOM, cut the cake during a ceremony commemorating the Navy Reserve's 96th birthday. (Left) Navy Cyber Forces Deputy Commander Reserve Component, RDML Gordon Russell, delivers remarks at the ceremony. (Photos by Robin D. Hicks)

Deputy Commander Reserve Component, RDML Gordon Russell, who highlighted the history of the Navy Reserve and the current efforts to fully integrate the active and Reserve forces within the Navy's Information Dominance Corps (IDC).

"The embedding of the Reserve IDC communities within Navy Cyber Forces will bring responsibility to man, train, professionally develop and deploy more than 6,000 Reserve Sailors, resulting in the creation of a true Total Force Type Commander," Russell said. "These men and women deserve our sincerest appreciation for their service. They are making history today that future Navy

Reserve birthday celebrations will commemorate."

On hand to cut the ceremonial cake were CAPT Doug Swanson, assistant chief of staff for Network Operations, NETWARCOM and YN2 Kassiana Earp, Flag Writer for the NETWARCOM commander. Swanson and Earp represented their fellow Navy Reservists serving at the two commands, as the oldest and youngest members currently on board.

For more information on Navy Cyber Forces and Naval Network Warfare Command, visit the commands' Navy News Web pages at www.navy.mil/local/ncf and www.navy.mil/local/nnwc.

CYBERFOR Welcomes New Deputy Commander

F. Scott DiLisio recently reported to Navy Cyber Forces as Deputy Commander. In this capacity, he serves as deputy and principal advisor to the CYBERFOR Commander on all matters relating to Navy C5I programs and requirements.

DiLisio's career with the Federal service has spanned 24 years, and he was appointed to the Senior Executive Service in 2006. His previous SES assignments include serving as Executive Director, Submarine Forces where he was the principal advisor to the Submarine Force Commander on all matters relating to Undersea Enterprise programs and requirements. He also served as Assistant Deputy Commander, Fleet Logistics Support at Naval Sea Systems Command (NAVSEA), with responsibility for program management and implementation of logistics functions, policies and processes within NAVSEA and its field activities.

DiLisio began his professional career with the Department of the Navy in 1987 as a logistics management specialist in the office of the Chief Engineer for Logistics at Naval Sea Systems Command. In September 1989, DiLisio was selected as the Integrated Logistics Support (ILS) manager for the AOE-6 Fast Combat Support Ship, where he was charged with the complete re-planning effort and execution of the full ship class logistics program. He directed the ILS delivery of the first two ships of the class.

In 1994, he was appointed Logistics Director of the Strategic Sealift Program. Under his direction, the Strategic Sealift Conversions and two lead new construction ships were successfully delivered into service.

In May 1998, DiLisio was appointed as the Director of Operational Readiness for the DD-21 program where he was responsible for devising new, innovative logistics strategies for the support of the U.S. Navy's newest destroyer class.

He also served as the Deputy Program Manager for the restructured DD(X) program. As the senior civilian in charge of the ACAT ID 21st Century Destroyer program, DDG 1000, he directed the successful execution of a



F. Scott DiLisio

\$2.9 billion phase III effort.

DiLisio holds a Bachelor of Science degree in Business Administration from Strayer University. He is a recipient of numerous professional awards including multiple Superior Civil Service Awards. He is a member of the Acquisition Professional Community.

Navy Steps Up Protection of Sailors' Information

From Navy Personnel Command Public Affairs

MILLINGTON, TN -- To comply with a Department of Defense directive aimed at protecting Sailors' personal information, Navy Personnel Command (NPC) will change the method for posting official messages containing partial Social Security Numbers (SSN) on its public website.

"All messages to be reviewed were pulled from the Web in December (2010), and NAVADMINS from 2009 and 2010 were scrubbed of personally identifiable information (PII)," said NPC Webmaster Don Koehler. "We reposted the recent ones to the 'NPC Messages Page' after the partial SSNs were removed."

According to Koehler, messages from 2008 and earlier that contain PII are not being reposted. These include selection and promotion messages dating back to 2000 that contain partial SSNs and had been available online for many years. Visitors to the public website, www.npc.navy.mil, attempting to open these messages will receive the following response:

"The message you have requested has been removed due to a Nov. 23 OSD (Office of the Secretary of Defense)

directive prohibiting the posting of the last four digits of a person's social security number on public facing websites (OSD 13798-10)."

"This change is a safeguard directed by the Office of the Secretary of Defense in directive 13798-10," said Koehler. "Specifically OSD ordered that 'Social Security Numbers shall not be posted, in whole or in part, on any public-facing and/or open government website in any form.'"

Beginning in 2011, selection and promotion messages will be posted without partial SSNs. Given that there is the potential for service members with the same name to be up for the same selection or promotion board, Sailors may go to BUPERS Online to check their personal selection or promotion status.

Access the 'NPC Messages Page' at <http://www.npc.navy.mil/ReferenceLibrary/Messages>.

To access pre-2009 messages that have been removed for PII, or for other questions about this change, call the NPC Customer Service Center at 1-866-U-ASK-NPC (866-827-5672). ✕

Space Education Building Ground Breaking Held at Peterson AFB

From 21st Space Wing Public Affairs

PETERSON AFB, CO -- After nearly six years of operating at an off-base location, the Space Education and Training Center (SETC) broke ground for its new \$14.4 million facility near Colorado Springs, Dec. 10. The state-of-the-art training and education facility will house four organizations:

- The National Security Space Institute (NSSI), which is part of Air University's Ira C. Eaker Center for Professional Development.
- The Reserve component to NSSI, under the 310th Space Wing.
- Advanced Space Operations School (ASOpS), belonging to the Space Innovation and Development Center.
- A Navy Cyber Forces detachment.

Moving the campus to a military installation resolves force protection and academic operations concerns with the current off-base facility. The anticipated move-in date is set for fiscal year 2012.

In attendance at the ground breaking was Air Force Maj. Gen. Michael Basla, Air Force Space Command vice commander.

"It's been almost 10 years since the release of the Space Commission Report, which concluded there was a need to 'create and sustain a cadre of space professionals' and for the nation to 'place a high priority on intensifying investments in career development, education and training,'" said Basla.

The vice commander also attributed the groundbreaking as

symbolic for several reasons, most notably because "it signifies the need to train as we fight; not only as joint warriors, but as warriors in domains where the lines between space and cyberspace are becoming blurred."

Air Force Col. Stephen N. Whiting, 21st Space Wing commander, said the 21st Space Wing -- America's space superiority wing -- is the right host for the two schools, which are tremendous assets to today's space operators.

"As the host command, the 21st Space Wing is proud to welcome NSSI and ASOpS to Peterson Air Force Base," Whiting said. "We look forward to supporting their education of today's warrior Airmen in the realm of space."

Since 2004, the SETC has operated



(Above) A groundbreaking was held Dec. 10 for the new Space Education and Training Center on Peterson Air Force Base. The \$14.4 million facility will house the National Security Space Institute and Advanced Space Operations School. The center will be Air Force Space Command's state-of-the-art training and education facility for space professionals. Breaking ground (left to right) are James Moschgat, associate dean of Operations, NSSI; Col. Roger Vincent, Space Innovation and Development Center commander; Maj. Gen. Michael Basla, AFSPC vice commander; Col. Stephen Whiting, 21st Space Wing commander; Col. Mark Hustedt, 310th Space Wing vice commander; and Navy CAPT Raymond Ginnetti, Navy Cyber Forces Colorado Det. senior officer. (U.S. Air Force Photo by Rob Bussard)

from a leased commercial facility in Colorado Springs because adequate on-base facilities did not exist anywhere within the region. While the current facilities are suitable, they were designed for business use, not specifically to promote academic excellence.

In addition, the current home does not meet all the force protection criteria a DoD agency requires to operate in a post-9/11 world. The new SETC campus will provide an ideal environment for higher learning while eliminating current force protection concerns and afford the staff, faculty and students ready access to Air Force Space Command and Peterson



AFB's resources.

The building and some other support functions will be run by the ASOpS.

Each year, ASOpS provides advanced training to more than 1,600 DoD space professionals, while NSSI, the Air Force's space professional development school, provides first-class education to more than 800 space professionals annually.

"You are the key to our nation's investment in the next generation of space professionals," said Basla, "as we continue to break ground in the way we train and educate our space warriors for tomorrow's joint fight." ✕

LETTERS FROM THE SEA

Greetings from La Union, El Salvador

This is day 103 of Southern Partnership Station 2011 (SPS), with 53 left to go. So far, the mission aboard High Speed Vessel Swift (HSV 2) has taken us to port calls in Port-au-Prince, Haiti; Concepcion and Valparaiso, Chile; Callo Peru; Manta, Ecuador; and Puerto Quetzal, Guatemala. After El Salvador, we stop in Honduras and Nicaragua with a second humanitarian supply drop in Haiti before returning stateside April 8.

Our first supply drop in Haiti came last Nov. 8, just days after Tropical Storm Tomas hit the island. We took medical supplies, water filtration units and a mobile medical bus -- it couldn't have been more timely.

SPS 2011 is all about partnering with the places we visit: subject matter expert exchanges with security and medical experts, cross-training with Marines, and partnering with host nation Navy construction teams as we renovate and build structures to make life better for people in Latin America. Of course, we also have humanitarian assistance supplies provided through Project Handclasp, a non-government agency that partners with the Navy to deliver assistance on a space-available basis aboard our ships. By the end of each port call, the people we've interacted with



(Left to right) High Speed Vessel SWIFT (HSV 2) Master, Capt. Nick St. Jean; HSV 2 Military Det. OIC, LCDR Chris Simmons; SPS 2011 Mission Commander, CDR Mark Becker; Guatemalan President Alvaro Colom; SPS 2011 Foreign Affairs Officer, Air Force 1st.Lt. Axel Zengotita; SPS 2011 PAO, MCC(SW/AW) Aaron Strickland pose for a group shot after dining together. (Official U.S. Navy Photo)

universally show big smiles and thanks for Americans coming to their country and lending our support.

Unlike most Navy ships, Swift spends most of its time in port, not at sea. We sail for a day or two, then spend two or three weeks at each port. Swift is a civilian owned high-speed catamaran cargo ship leased to the Navy. It's navigated, engineered and maintained by 17 civilian contracted Merchant Marines. Another 20 Sailors are assigned as administrative assistants with the ship and its mission. The remaining 65 Sailors, Marines and Airmen staff SPS 2011 on a TAD basis and will return to their parent commands after April 8. The ship and the mission are unclassified -- a Web search yields a nice picture of the ship and her capabilities.

Our port calls have been fascinating. El Salvador has beautiful vistas at its port in La Union: mountains with purples, blues, pinks, browns, greens, and a deep blue-green bay.

The weather is quite warm - sunny and near 90 degrees with a lot of humidity. It's easy to cool off -- just step out of direct sunlight and a breeze will do the trick -- but, it only takes a minute or two to feel like you're overheated in the tropical sun.

Guatemala is much the same ... hot and humid. While in Puerto Quetzal (the port for San Jose), there were a few opportunities to eat out. My first was on my birthday lunch at the officer's mess on base.

Pacayu is an active volcano about 20 miles east of San Jose, located in a national park. The hike is 2.3 kilometers (about 1.5 miles) up a steep trail up to the top of the tree line. The "old" cone is just above the tree line and from there you can see the "new" cone that erupted last May, which is a good 500 feet higher. It was venting steam and gas the day we visited. We skidded down a sheer drop a few hundred yards from the old cone onto the lava field from last May's eruption.

The lava field was still hot in a few places; people bring hot dogs and roast them over one of the vents in the field. From the field, you get breathtaking vistas into Guatemala City 20 miles away to the east and back to the west to the port as well as to other, taller volcanic mountains farther away in the range.

Berthing Swift beside a naval base in Guatemala

allowed us the luxury of coming and going on the base as we pleased, and it came with a bit of extra security because the president's weekend retreat house was across the parking lot from our ship. Our second Saturday in port, President Colom arrived via helicopter, walked over to the foot of the brow and invited the mission commander to breakfast Sunday morning. As I stood there snapping a few shots, he turned to me and said "well I need someone to take a few pictures," and just like that, I was eating breakfast the next morning with the president!

President Colom was quiet-spoken and casual. We enjoyed a nice chat about what he has done and hopes to do with Guatemala in the 12 months left in his term. He impressed me as a man with a dream about helping his country.

In South America we stopped in Manta, Ecuador, a small harbor town along the Pacific. This is their major harbor, although its size would fool you. A big chunk (no pun intended) of the world's tuna is caught just off its shores. Being a smaller town, there weren't as many liberty opportunities, but the nearby naval base opened its doors to us on two straight Fridays for a cookout and soccer. We celebrated the New Year there, and were amazed by the hundreds and hundreds of fireworks launched at midnight. Most of the fireworks looked to be the size that would only be fired by professionals in America.

In Callao, Peru, and between subject matter expert exchanges and construction projects, we enjoyed Miraflores, a major tourist community within the capital city of Lima, a metropolis of nearly seven million people. Miraflores has lots of extra police patrols, making it very safe and secure for time off. At the oceanfront (which is a 200-foot high cliff), they've built a shopping center that opens over the ocean. You walk down two flights of stairs from street level to enter the mall. From the street, the mall is more or less invisible; just a park along the cliffs with some stairs going down. The entire ocean side of the shopping center is glass with restaurants overlooking some spectacular views. The mall and Miraflores has a lot

... continued on Page 14

Graphic Illustration by MC2(SW) Joshua J. Wahl

of nice restaurants that didn't charge an arm and a leg to eat there.

Some of the crew exchanged Christmas presents in Peru as we celebrated Feliz Navidad. Again, lots of fireworks at midnight on Christmas Eve. Amazing.

Our port calls in South America began in Concepcion, Chile, painting houses their Navy had built as temporary housing after their devastating earthquake in 2010. It felt good to pick up a brush and make their houses look a bit more like a home. Dozens of Sailors went out each day to help, too. After painting, we'd use off-time there and in Valparaiso (and its neighbor, the gorgeous beach resort of Vina del Mar) to visit their shopping malls.

At Valparaiso, Chile, we were the featured U.S. Navy ship for Expo Naval 2010, a week-long major South American event to showcase naval technology. Navies from as far away as China and England sent representatives. Two days in a row, Swift carried some very happy guests on a one-hour harbor tour.

Throughout the mission, we've found that shopping here is remarkably similar to home. We have found a lot of local cuisine in their food courts, but a surprising amount of American food, too. In Guatemala, for example, a popular American pizza chain delivered to the gate, and our van drivers would collect it (in exchange for a slice or two, of course) and bring it onto the ship.

We've had a lot of opportunities to share the goodwill of America with some very hospitable hosts in Latin America on SPS

2011, and you can be certain that we've established a lot enduring friendships as we've carried the flag up and down the Pacific coast. It's been rewarding, but everyone is starting to feel the tug of our homes and our families calling us back. See you there soon! ✂

EDITOR'S NOTE: MCC(SW/AW) Aaron Strickland is currently deployed on a temporary duty assignment as the Public Affairs Officer, Southern Partnership Station 2011, aboard High Speed Vessel Swift (HSV 2). In his primary billet, he serves as Leading Chief Petty Officer and Press Chief for Navy Cyber Forces Public Affairs.



(Above) Sailors assigned to HSV 2 Swift paint houses during a community relations project supporting Southern Partnership Station (SPS) 2011. The 25 Sailors and Marines embarked aboard HSV 2 painted more than 20 homes during the week-long project in Concepcion, Chile. (Photo by MC2 Ricardo J. Reyes)



(Left) HSV 2 Swift leaves another South American port during SPS 2011. The annual event deploys U.S. ships to the U.S. Southern Command's area of responsibility in the Caribbean and Latin America. During its 156-day deployment HSV 2 Swift made port calls in Port-au-Prince, Haiti; Concepcion and Valparaiso, Chile; Callo, Peru; Manta, Ecuador; and Puerto Quetzal, Guatemala. (Official U.S. Navy Photo)

NIOC Georgia Chief Adds to His Paralympic Achievements

By George D. Bieber, CYBERFOR Deputy PAO

CHRISTCHURCH, New Zealand — The American men were not shut out on day four of the 2011 International Paralympic Committee (IPC) Athletics World Championships thanks to a bronze medal in the long jump won by CTIC Casey Tibbs from Navy Information Warfare Command (NIOC) Georgia. Tibbs landed a jump of 6.19 meters to secure a spot on the medal stand, where he accepted his third medal in the IPC Championships since winning a gold and silver medal in 2006.

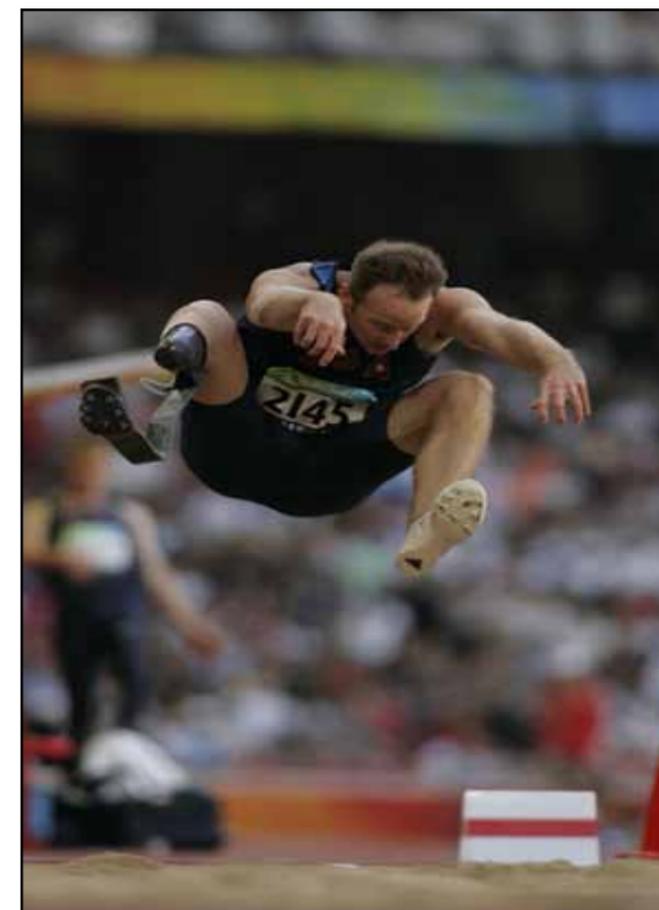
"I've now competed in two Paralympic Games, three World Cups, and this was my second World Championships," said Tibbs. "Getting out on the track and competing against the world's greatest athletes while wearing USA on my chest will never get old. This year's USA World Championships team was filled with talented athletes, patriots and even a few veterans."

The 30-year-old Sailor made history in 2004 by becoming the first American active-duty military member to compete in a Paralympic Games. He topped off that achievement with two medals: silver in the pentathlon and gold in the men's 4 x 100 meter relay. At the 2008 Paralympic Games in Beijing, China, he captured gold in the 4 x 100 meter relay and a bronze in the long jump.

"This year has been very busy for me, but one of the most important years of my life," said Tibbs. "We

celebrated the birth of my daughter, my promotion to Chief Petty Officer and the journey of life's lessons which I continue to learn everyday from Sailors!"

2011 also marks the 10 year anniversary of the amputation of Tibbs' right leg below the knee,



CTIC Casey Tibbs reaches for air during his 6.19 meters long jump at the 2011 IPC Athletics World Championships. Tibbs took a bronze medal in the event. (Photo by Frank Polich Photography)

following a motorcycle accident in March 2001 at Goodfellow Air Force Base, TX.

"These past 10 years have been amazing and I've gotten to see so

many things and places that most don't see in a lifetime," reflected the Navy veteran of 11 years. "It was the Navy that showed me this path, the Navy encouraged me to be successful with my physical disability and it was the Navy that took a chance on me allowing me to stay on active duty. Little did I know of the example that I was setting."

The San Diego native has been at NIOC Georgia since graduation from Navy Aircrew Candidate School in June 2009. Tibbs is the first amputee to complete Navy Survival Evasion Resistance and Escape training, as well as the first amputee to become an Aircrew man through the U.S. Navy Aircrew School.

"Every command I've ever been at has been extremely supportive of my Paralympic endeavors," said Tibbs. "However, I still deploy and take on all tasks the Navy brings upon me. Training takes place whenever I get the chance. There is always downtime during these world sporting events, and it's the most vital time for athletes to mentally prepare for competition, a time when one can look at how ready they are to compete."

The father of two, with another one on the way, finds deployments to be the best opportunity to train, except there usually isn't a long jump pit to

... continued on Page 16



(Far Right) CTIC Casey Tibbs joins gold and silver medalists in rendering honors during the 2011 International Paralympic Committee (IPC) Athletics World Championships. Tibbs took a bronze medal in the long jump competition. (Photo by Frank Polich Photography)

When confronted by media in New Zealand, the day before he took a bronze medal in the men's long jump, Tibbs had this to say, "I am facing some tough competition tomorrow, some of the toughest I've ever faced. I love to compete and I know that I always give my best every competition. Life on the track is same as life in the Navy; if we always give our best we will get the job done. Never Give Up!"

"Being a chief in the U.S. Navy and competing for Team USA, I wear a uniform all the time," said Tibbs. "We have a motto that says, 'A chief always has to be ready,' and given that I was deployed twice last year and

didn't have as much preparation as I would have liked, I knew I still had to be ready to compete. Coming away from world championships with a bronze medal is a definite win."

There were a few other military veterans who also competed in New Zealand; however, none of them were active duty. With more than 30,000 Wounded Warriors from Operations Enduring Freedom and Iraqi Freedom, there are many who are now training and starting to qualify for Paralympic sports. In fact the Defense Department's inaugural Paralympic Warrior Games will be held in Colorado Springs, CO, May 10-14.

Follow the U.S. Paralympic team throughout the year at www.USParalympics.org.

train in.

"I always wish I had more time to train," he added. "Being a veteran in the spotlight I know what it takes to train properly. I also have a coach, Joaquim Cruz, who I can call and get good advice from. He was my coach when I was stationed in San Diego and taught me a lot about fitness and how to prepare."

Tibbs has been competing in track and field since he was 12 years old and from his sophomore through senior year in high school he was on the Varsity track, football, golf and soccer team. The Chief has been on the U.S. Paralympic track and field team since 2003 and he plans on competing for as long as he can keep qualifying for the U.S. team. "I truly enjoy competing and it's a great way

to stay motivated," said Tibbs. "I have been in the Navy for nearly 12 years and I am making a career out of the World's Finest Navy!"

Tibbs' wife and children are his strongest supporters in any of his endeavors. They understand when he deploys and they understand how much it means to both him and the Navy to compete on the U.S. Paralympic team.

"A lot of Sailors ask me how I get to go compete or how I got to stay in the Navy after losing my leg," said Tibbs. His advice is always short and simple, "Don't Give Up! No matter what you might go through, you have to move on. And if there is something you want to do, and it's within good standing of our core values ... Ask your Chief!"

CTIC Casey Tibbs' Achievements:

- 2011: Bronze medal, long jump - IPC Athletics World Championships, Christchurch, New Zealand
- 2008: Gold medal, Men's 4 x 100 meter relay; bronze medal, Long Jump - Paralympic Games, Beijing, China
- 2007: Excellence in Sports Performance Yearly Award Recipient, Best Male Athlete with a Physical Disability
- 2006: Gold medal, pentathlon; Silver medal, long jump - 2006 IPC Athletics World Championships, Assen, The Netherlands
- 2006: Named U.S. Olympic Committee September Athlete of the Month
- 2006: First place, long jump; third place, pentathlon - 2006 U.S. Paralympics Track & Field National Championships, Atlanta, GA
- 2005: Deployed to Afghanistan in support of Operation Enduring Freedom
- 2004: Gold medal, 4 X 100 meter relay; Silver medal, pentathlon - Paralympic Games, Athens, Greece
- 2004: Second place, 400 meter - Paralympic Exhibition Race, U.S. Olympic Trials, Sacramento, CA
- 2004: U.S. Olympic Committee Paralympic Athlete of the Year Award
- 2004: Named Federal Employee of the Year with a Disability by the National Security Administration
- 2003: First place, 100 meter, 400 meter - Endeavor Games, Edmond, OK
- 2003: Second place, 400 meter - Rocky Mountain State Games, Colorado Springs, CO

MWR Funds Allow Military, Retirees & Eligible Family Members Usage of Safari Books

Online

From DoD Public Affairs

Safari® Books Online www.safaribooksonline.com, the leading on-demand digital library for technology, digital media and business professionals, has been chosen by the Department of Defense (DoD) to provide eligible active and retired military personnel and their family members with access to thousands of books via their designated service portal: Army Knowledge Online (AKO), Navy Knowledge Online (NKO), Air Force Portal (AFP), or MilitaryOneSource.com

The complimentary access to Safari® Books Online is realized by funding appropriated by Morale, Welfare and Recreation.

Access to Safari® Books Online makes it easy to solve challenges, enhance knowledge and professional skills, quickly and easily search for reliable, definitive answers to mission-critical questions, and stay on the cutting-edge of your profession or hobby.

Subscribers use Safari®Books Online's robust database and sophisticated search engine to quickly pinpoint specific information on topics such as technology skills and certifications, programming, cloud computing, Excel, Word, PowerPoint presentations, project management, Web development, digital photography, iPod, iPad & iPhone use, business management and leadership, social networking, financial advice, Java development and more.

- Easily and quickly access thousands of current and relevant resources.
- Stimulate creativity and enhance professional and personal growth.

The product is packed with features that make the reading experience enjoyable and help ensure an interactive learning experience. Features such as online note taking, highlighting on screen, bookmarking and creation of printable note summaries provide you with the tools to help you categorize and use expert resources in a variety of formats from the world's leading publishers. Safari® contains more than 1,000 training and instructional videos as well as more than 14,000 of the top technology and business books.

Not only are trees being saved by providing all this great information in digital format, but Safari® Books

Online also provides the ability to take the library with you – off line in a PDF or on a mobile device m.safaribooksonline.com.

Visit your DoD Service Portal at AKO, NKO, AFP, or Military OneSource and register for a Safari® Books Online ID and password to find answers to critical questions today! Once registered, you will receive an email from Safari® Books Online that explains how to access the Safari® Books Online library directly. Once logged into Safari®, you can browse the content or create simple or advanced searches to find the information you are looking for.

If you have additional questions, contact us at: dnaon@safaribooksonline.com or call Denise Nason at (910)-233-2435. ✂

About Safari® Books Online

Safari® Books Online www.safaribooksonline.com is an on-demand digital library that delivers expert content in both book and video form from the world's leading authors in technology and business. Technology professionals, software developers, Web designers, and business and creative professionals use Safari® Books Online as their primary resource for research, problem solving, learning and certification training. Safari® Books Online offers a range of product mixes and pricing programs for organizations, government agencies and individuals. Subscribers have access to thousands of books, training videos and prepublication manuscripts in one fully searchable database from publishers like Cisco Press, Prentice Hall Professional, O'Reilly Media, Addison Wesley Professional, Microsoft Press, Sams, Que, Peachpit Press, John Wiley & Sons, Elsevier, IBM Press, Adobe Press, Sun Microsystems Press, FT Press, Wharton School Publishing, Apress, Manning, New Riders, Apple Certified, Course Technology, Splash Media and dozens more. For more information about Safari® Books Online, please visit us online at: www.safaribooksonline.com.

Graphic Illustration by MC2(SW) Joshua J. Wahl



NIOC Whidbey Island Sailor Receives Award

By CTR1(IDW/NAC/AW/SW) Cris Dominguez, NIOC WI Public Affairs

LTJG Sean Thompson was one of 21 awardees presented with the 2011 Copernicus Award at the Armed Forces Communications and Electronics Association (AFCEA) West Conference in San Diego, Jan. 24.

Thompson received the award in recognition for his accomplishments as a Weapons and Tactics Instructor, as well as for his work with the MCS-21 program. He is currently serving as the Command NATOPS Officer at Navy Information Operations Command (NIOC) Whidbey Island.

"I was excited to learn that I had been selected as a Copernicus Award winner," said Thompson. "Although this is an individual award, it is reflective of the work done by our Sailors at NIOC Whidbey Island on a daily basis." Recipients are selected each

year by judges in the sea services based on their sustained superior performance in a U.S. Navy,



LTJG Sean Thompson displays his award. (Photo by Dana Banta, NIOC WI)

Marine Corps, and Coast Guard Command, Control Computers, Communications and Intelligence/Information Technician (C4I/IT)-related job. AFCEA and the Naval Institute presented the awards.

AFCEA was established in 1946 as a non-profit membership association serving the military, government, industry and academia as an ethical forum for advancing professional knowledge and relationships in the fields of communications, IT, intelligence, and global security.

"I'm extremely pleased that AFCEA and the U.S. Naval Institute were able to appreciate LTJG Thompson's superb talents and performance in the same manner as I do daily," said CDR Joseph Pugh, NIOC Whidbey Island's commanding officer. "He embodies and delivers all that this award advocates; mission accomplishment and professional excellence."

Thompson's accomplishments included the development of new tactics, techniques and procedures for the utilization of emerging technologies aboard the EP-3E aircraft. He was also the driving force behind the integration of new technologies, to include having the lead role in the testing of mission systems that expand the aircraft's capabilities mission effectiveness.

Thompson enlisted in the Navy in 1996 as a Cryptologic Technician Collection and received his commission as a Limited Duty Information Warfare Officer in 2008 while aboard the USS Sampson (DDG-102). He has served in both the surface and aviation communities.

The Copernicus Award was established in 1997 by retired Air Force Lt. Gen. C. Norman Wood, then president and chief executive officer of AFCEA International, and the late Navy VADM Art Cebrowski. It is named after the 16th century Polish astronomer Nicholas Copernicus.

NCDOC Employee Chosen as 2010 Award Recipient

By ITC (SW) Tyree Scott, NCDOC Public Affairs Officer

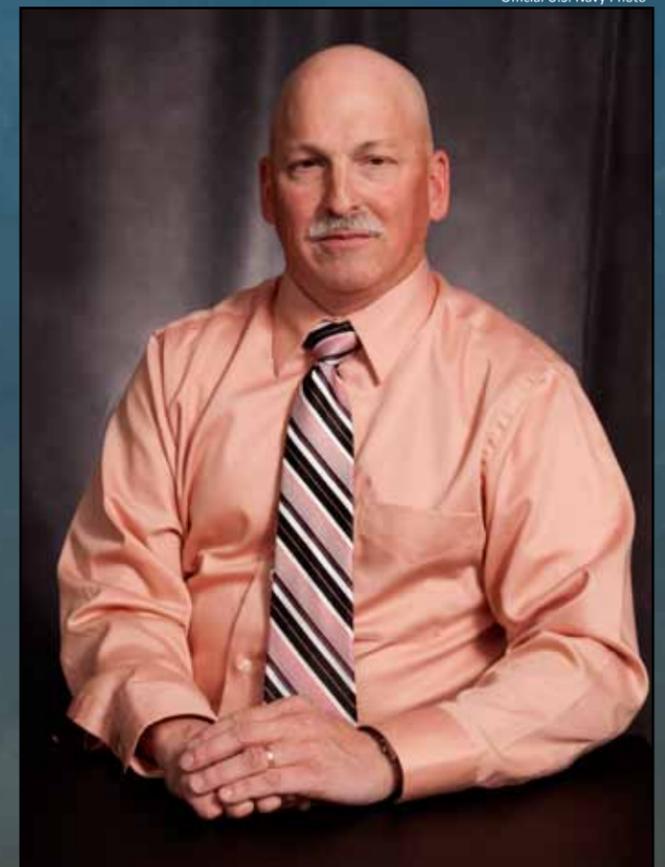
VIRGINIA BEACH, VA – The Navy recently selected 21 winners for its fiscal year 2010 Copernicus Award which included Navy Cyber Defense Operations Command (NCDOC) Capabilities and Readiness (C&R) Director, James Granger.

Granger spearheaded the development of a hierarchal data roll up capability to enable sharing of Host Based Security Suite (HBSS) event and asset data between the Navy and U.S. Cyber Command (USCYBERCOM). He was instrumental in providing the necessary briefs and point papers to Fleet Cyber Command/Commander 10th Fleet (FCC/C10F) and Naval Network Warfare Command leadership and was the driving force in the realization of this revolutionary architecture. Despite significant roadblocks and uphill struggles, this Navy-driven Department of Defense (DoD) solution is being considered for implementation by the other services due to the efforts of Granger and his personnel.

In a fiscally constrained environment, Granger continually challenged his team to fully leverage existing capabilities. Under his leadership, his directorate executed a deliberate plan to maximize utilization of the Navy's existing sensor capability that significantly reduced the time required for an analyst to identify infected computers. These and other actions resulted in the automated mitigation of more than seven million instances of unauthorized activity per day (approximately 55 percent of all alarmed activity Navy-wide) providing the Navy significant cost and manpower savings.

NCDOC is charged with defending the Navy's unclassified and secret computer networks. More than 280 military, DoD civilian, and contractor personnel fight the 'net' through aggressive detection and analysis of adversary cyber operations while directing proactive defense actions to counter threats. Granger is responsible for providing Navy enterprise Computer Network Defense (CND) capabilities to enable NCDOC to successfully execute its mission as the Navy's CND Service Provider (CNDSP) in support of FCC/C10F and USCYBERCOM.

The Copernicus award was established in 1997 and is named after the Copernicus Architecture (shifting the center of the universe) used as the blueprint for the future Command, Control, Computers,



NCDOC's C&R Director, James Granger.

Communications and Intelligence (C4I) structure of the Navy. Recipients are selected based on their sustained superior performance in a C4I/Information Technician-related job. The selections are made each year by Navy judges who review applications from the Navy, Marine Corps and Coast Guard, and include both active duty and civilian personnel.

The award is sponsored by the Armed Forces Communications and Electronics Association and the U.S. Naval Institute. Granger along with other winners was recognized at an award ceremony Jan. 25 in San Diego.

Graphic Illustration by MC2(SW) Joshua J. Wahl



Guest Speakers Embrace Technology & Cyberspace

By Jeff Ristine, U. S. Naval Institute

SAN DIEGO -- As the U.S. military emerges from 'the long war' of Afghanistan and Iran and confronts potential rivals around the world, a top naval official said it will become vital to master cyberspace and embrace technology that has yet to emerge.

"We need to look to the future and be bold," VADM Richard W. Hunt, commander, 3rd Fleet, said in the opening address at the Armed Forces Communications and Electronics Association (AFCEA) West 2011 conference at the San Diego Convention Center. "Go after the new technology, put stuff out there and be back into experimentation."

According to Hunt, threats to electronic technology need to be better understood and fixed. "They occur in many, many areas now," the admiral said. "... changing so fast we don't understand the vulnerabilities because we didn't design the systems."

Hunt also believes that protecting ourselves in the cyber world may be as important as any particular warfare area that we have out there. "If we lose our computers, if we lose our information exchange, the way we operate today cripples us completely," he said.

'After the Long War: What's Next' was the theme of the three-

day conference, co-sponsored by the U.S. Naval Institute and AFCEA International.

Confronting cyberspace issues are among a set of future challenges for the Navy that include violent extremism – a threat Hunt said is "here for a long time" – and competition for scarce resources, a challenge he associated with the rise of China and India.

"The constant in today's environment is rapid change that necessitates that we be agile and adaptable in all that we do," said Hunt. "We need to focus on the need to adapt to a changing environment."

The admiral spoke admiringly of touring ships from other nations that contained large empty spaces for unforeseen, future needs, an improvement on the Navy practice of uneconomically ripping out and replacing equipment instead of expecting the need for change.

And while it may not be feasible to construct a 'completely invulnerable wall' around essential computer infrastructure, Hunt said it is vital to understand when an attack is occurring. "Our ability to do the same to an adversary is equally important."

Graphic Illustration by MC2(SW) Joshua J. Wahl

More traditional vulnerabilities, however, shouldn't be neglected either, Hunt said. "We need to go back ... and make sure we plug those holes or you can attack us that way as easily, perhaps even easier, than you can through cyber attacks."

Without reference to the political landmines sometimes associated with the subject, Hunt also mentioned climate change as a long-term concern for the Navy. "What do we do if the water level rises, like some people predict that it will by 2040, by eight to maybe ten feet? What does that do to the San Diego waterfront? What does that do to the infrastructure of the U.S. Navy? It won't be insignificant."

In other highlights of the first day's programming:

Marine Maj. Gen. Melvin G. Spiese, deputy commanding general of the Camp Pendleton-based I Marine Expeditionary Force, told a luncheon audience the U.S. can never be complacent about the support it will receive around the world when vital interests are at stake. "We have seen nations change their policies over time as their interests change," he said. "We cannot expect that they will support us as a matter of fact."

A panel spoke enthusiastically of the potential from expanded use of unmanned systems, such as the drones in use in the skies above Afghanistan. "The Navy is making 'exciting' investments in such systems," said Dave Weddel, assistant deputy chief of Naval Operations for Information Dominance. They include an unmanned aircraft for carrier landings and air-to-air refueling, to be tested as early as next month.

"Unmanned systems improve the persistence and endurance of the Navy and its ability to go where you would not necessarily push the envelope with a manned

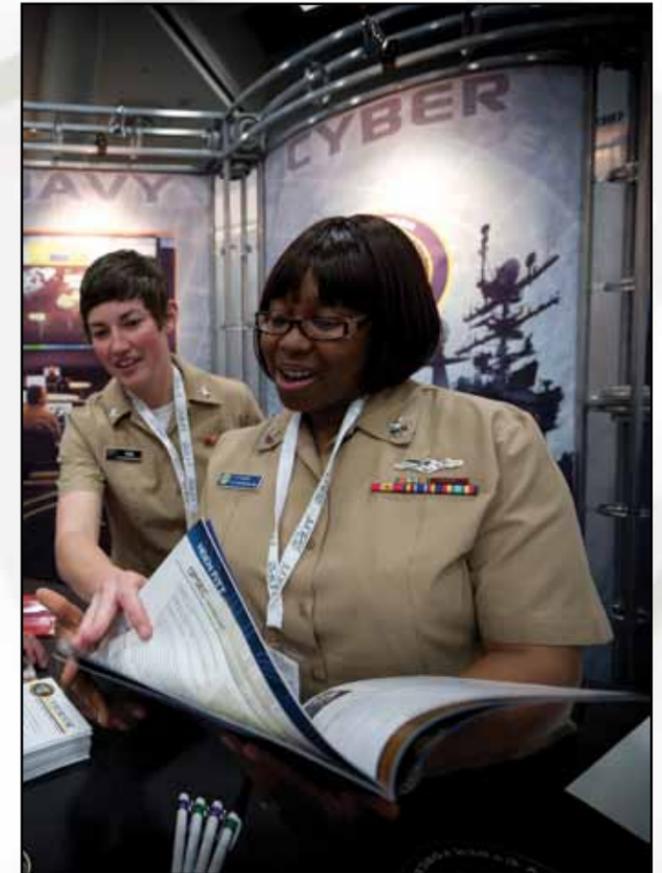
aircraft," Weddel said.

Within five or six years, use of unmanned systems for operations and surveillance will be so heavy the military will need to make sure it has invested enough to handle all the data generated by the systems.

"There's much that we have to do in terms of infrastructure," said Weddel, "and there's much that we have to do in terms of architecture."

EDITOR'S NOTE:

This article is reprinted from *Proceedings with permission; copyright (s) 2010 U.S. Naval Institute/www.usni.org.*



(Top, left to right) CTM3 Ashley Pfahl, NIOO Det San Diego and IT1(IDW) Jacquelyn Fitzpatrick, NCTS San Diego assist customers at Navy Cyber Forces' (CYBERFOR) booth at the AFCEA West 2011 conference in San Diego. (Above) ITCM(SW/AW) Gary Myers, CYBERFOR's SEA, greets visitors at the command's booth during the AFCEA West 2011 conference. (Photos by Robin D. Hicks)



(Left to right) Kent Schneider, AFCEA President/CEO; Amanda Jordan; Natalie Givans, AFCEA Chair of Board of Directors and Jordan's mother, Jan; pose after Jordan was presented the 2011 Virginia Region Young AFCEA award at 2011 AFCEA West conference in San Diego. (Official U.S. Navy Photo)

Corona Warfare Center's Patented System Wins Top Navy Award

By Troy Clarke, NSWC Corona Public Affairs

SAN DIEGO -- A team from Naval Surface Warfare Center (NSWC) Corona received a top Navy Information Management/Information Technology (IM/IT) Excellence Award at the 2011 D department of the Navy IM/IT Conference Jan. 25.

The team received the award for developing a calibration management system that is projected to save the Navy nearly \$65 million by 2017.

The system, called the Metrology Bench-Top, or METBENCH, was praised by the Navy's Chief Information Officer (CIO), Terry A. Halvorsen, who presented the annual award which recognized outstanding contributions by individuals and teams who are transforming the Navy and Marine Corps through information technology.

Halvorsen said that Corona's efforts were a great example of innovation, efficiency and effectiveness. "Calibration of equipment is very important in the fleet," emphasized Halvorsen. "This system will increase mission effectiveness while decreasing our expense."

Calibrations are critical to nearly every aspect of naval operations and helps ensure equipment functions properly and accurately, ranging from a ship's propulsion plant to an F/A-18 Hornet's laser target designators to night vision goggles.

METBENCH program manager Richard Schumacher said the system seamlessly integrates more than 136 automated calibration procedures for 835 items across NAVSEA's calibration footprint. "This significantly increases calibration efficiency and improves equipment availability for the Navy's 1.85 million pieces of test equipment needed to conduct about 800,000 calibrations per year," Schumacher said.

He said Corona developed the cost-saving system in response to a fleet request in 2006 to address calibration systems that were ending their lifecycle. The METBENCH team took the unique system from concept to sea trial within 12 months and completed installation for the surface fleet last September. The system is currently aboard 144 surface ships.

Schumacher added that Corona's approach to shipboard calibration fully utilizes the Navy's distance support architecture to best support the fleet deployed anywhere in the world, and the METBENCH system makes these tasks as easy and transparent to the Sailor as possible.

The new single system replaces five existing IT systems scheduled to be phased out and provides Navy information management for more effective decision making, improved efficiency of tasking, as well as enhanced mission effectiveness, program managers say.

The METBENCH system relies entirely on open-source and government off-the-shelf technology and consists of several integral components, such as automated procedure execution; advanced calibration procedure development; and both afloat and ashore calibration asset management. Program managers say these key



DON CIO Terry A. Halvorsen, left, congratulates Dr. William Leubke, technical director for NSWC, Corona Division, after presenting the DON IM/IT Excellence Award to NSWC Corona METBENCH team during the AFCEA West 2011 Conference. (Photo by Greg Vojtko)

elements complement one another and help align Navy systems commands, fleet users, technical agents, type commanders and ashore calibration activities.

In conjunction with the surface fleet roll-out of METBENCH, NAVSEA began to install the ashore portion of the system in fiscal year 2010 at several calibration laboratories. The full system capability, including the lab management function, will be up and running at all NAVSEA enterprise calibration laboratories during fiscal years 2012-2014. The ashore automated calibration capability has already improved efficiency for the Navy by \$1.2 million.

Halvorsen says Corona's approach is exactly what the Navy needs and why the METBENCH team received the award.

"You've got more effectiveness, more efficiency. That's a win-win scenario," Halvorsen said. "And it's innovative. It's showing what can be done when people think a little outside the box. The NAVSEA example of that is a classic."

The award-winning Corona team members include John Griffith, advanced measurements program manager; Richard P. Schumacher, METBENCH/MCMS program manager; Juliusz Adamczuk; Zaide Figuerres; Jeff Walden; Rey B. Cheesman; Winston Y. Chou; Luis A. Cortes Jr.; Brett A. Currier; Stephen V. Frankini; Jeffrey M. Frappier; Michael L. Genung; Jeffrey M. Greene; Catherine F. Jose; Edvin Khanlarian; David G. Kinkade; Scott Jackson; Lawrence S. Lichtmann; Jeff Margosian; Vartan Nazarian; David B. Stice; Marisa Villasenor; Jove F. Yambot; Gary G. Yeakley and Zarch Zakarian.

EDITOR'S NOTE: NSWC Corona, a NAVSEA field activity, is responsible for gauging the warfighting capability of weapons and integrated combat systems, through assessment of systems' performance, readiness, quality, supportability and the adequacy of training.

For more news from NSWC, Corona Division, visit www.navy.mil/local/nswccorona/.



Navy COOL Wins at 2011 Human Capital Management Defense Awards

By Gary Nichols, CID Public Affairs Officer

PENSACOLA, FL -- The Navy Credentialing Opportunities On-Line (COOL) program won first place during the fifth annual 2011 Human Capital Management Defense (HCMD) Awards ceremony in Arlington, VA, Feb. 16.

The Navy swept through the HCMD awards with a total of three first-place wins, including the first place finish for Navy COOL.

Sharing the winner's podium for first place with Navy COOL in the "Best Workforce Development Program" category was the Navy's Fleet Readiness Center (FRC) East Wage Grade Development Programs Center of Excellence.

Also coming up with a first place win in the "Most Innovative Recruiting Program" category was Naval Sea Systems Command for its Wounded Warrior Recruiting Program.

"The Navy did exceptionally well," HCMD Event Production Executive Director Lisa Ringlen said. "I am very proud of all of our finalists and winners."

Approximately three million people work for the Department of Defense (DoD), making it the largest employer in the United States. As the nation's largest employer, managing people is an ongoing challenge and a top priority.

The HCMD organization has brought stakeholders from the Defense and Intelligence communities together to discuss, develop and recognize best practices for managing human resources.

HCMD developed an annual awards program five years ago to honor, recognize and promote the organizations from DoD and the federal government, which have developed and executed those best practices.

Pamela L. Spearow, director, Civilian Personnel Programs, U.S.

Naval Facilities Engineering Command Headquarters, served as one of the HCMD awards judges. She praised the Navy COOL program because of the direct benefits it offers to Sailors.

"Credentialing is a really big deal these days," Spearow said. "I really like this program because ... this credentialing process gives marketability to a military individual, especially when they get out of the military."

Navy COOL is a centralized, Web-based hub that consolidates information from numerous sources at the federal, state and local levels on certifications, licenses, apprenticeships and growth opportunities that correspond with each Navy rating, job and occupation.

The program has provided funding for Navy enlisted personnel to obtain civilian licenses and certifications that are closely aligned with a Sailor's job or rating.

Since its 2006 launch at the Center for Information Dominance (CID) Corry Station in Pensacola, FL, Navy COOL has processed more than 43,000 credentials for Sailors and received more than 80 million hits to the Navy COOL Web site at <https://www.cool.navy.mil>.

"I feel this award is a validation that the Navy's program is focused on the Sailor, the workforce, and in general the health and happiness of the Sailors," Navy COOL program manager Keith Boring said. "It means that not only industry, but that DoD can see that the Navy does have the right mix of training for its folks, both personally and professionally."

This year's finalists came from offices and programs from across the federal government,

representing the Army, Navy, Air Force, Coast Guard, Defense Information Systems Agency, Internal Revenue Service, Department of Energy, National Park Service and the United States Postal Service.

"For a program that's only been in existence for three years, receiving this kind of recognition at this level is huge," Navy COOL Director Sam Kelley said.

"DoD understands the linkage between what our Navy military performs and its association with the civilian counterpart, and the ability to transition using Navy COOL and credentialing to help fill immediate gaps within the Department of Labor requirements."

Perhaps just as impressive, Boring said, is the high pass rate of 96 to 98 percent for voluntary licenses and certifications among Sailors, compared to the national average pass rate of 75 to 80 percent.

EDITOR'S NOTE: CID is the Navy's Learning Center that leads, manages and delivers Navy and joint force training in information operations, information technology and cryptology.

With a staff of more than 1,050 military, civilian and contracted staff members, CID Corry Station oversees the development and administration of more than 168 courses at 16 learning sites throughout the United States and in Japan. CID Corry Station provides training for more than 19,000 members of the U.S. armed services and allied forces each year.

For more news from Center for Information Dominance, visit www.navy.mil/local/corry/.

PAGE CONTENTS

- Civilian Equivalent
- Certification - Advanced
- Apprenticeship
- Continuing Education

[Top]

New Rating:

▼



First CID Students Graduate From ITOF Pilot Course



By ISSN Shaun Sandbloom, CID Public Affairs

PENSACOLA, FL – Center for Information Dominance (CID) Corry Station held a ceremony in November 2010 for the Navy's first graduating class of the newly established Information Systems Technician of the Future (ITOF) course.

ITOF was conceived in response to Department of Defense (DoD) Directive 8570.01-M, which called for an DoD-wide solution to train, certify and manage the Information Assurance workforce in response to the ever-increasing cyber threats against networks based not only in the Department of Defense, but critical systems throughout the United States.

President Barack Obama recognized the importance of cyber protection and instituted measures to protect vital assets.

"Our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack," the president said in a May 2009 speech at the White House regarding the nation's cyber infrastructure. "Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country – attacks that are harder to detect and harder to defend against."

In response to the ongoing cyber threat to national

security, the president created a cyber security position in the National Security Council and ordered the creation of DoD Directive 8570.1. The new directive also requires technicians and managers to be trained and certified in specific fields.

"Our primary focus was to take care of the requirements and burdens in order to administer the IT rating professionally and adapt our rating to the 21st century," said ITOF Lead Instructor IT1 James Dise.

One of the main components of the new directive is that everyone with access to privileged systems will be required to have traceable and verifiable IT certifications in order to retain his or her job.

CID Corry Station's solution in ITOF has gone one step further to ensure that such education happens early in a Sailor's career, establishing an unprecedented understanding of cyber warfare against global threats.

The ITOF pilot class consisted of 20 students, who received a pre-graduation pep talk from CAPT Gary Edwards, CID commanding officer, Nov. 18 on board Corry Station.

"Our mission here is to train Sailors in skills necessary to save lives," Edwards said. "Make no mistake, we are fighting a digital war, not just on the frontlines in

Afghanistan, but here at home we are faced daily with the pressing need to enforce and reinforce our role in Information Dominance. The ITOF training you have just completed is integral to that process."

The success of the ITOF course keeps naval cyber forces on the cutting edge of an ever-evolving technological environment. With rapid and dynamic changes in technology, the Navy has been presented with the challenge of keeping their information technology community up to speed on the world around them.

"The program is definitely improving the Navy and the IT rate," Dise said. "There are so many opportunities in the Navy available to Sailors just for being an IT and being a part of ITOF."

Those future opportunities are the product of a long and arduous course, compressing several topics into a condensed, 19-week program. Furthermore, the certifications awarded for completing ITOF require a comprehensive understanding of administrator level information technology skills, elevating the educational prowess necessary to succeed.

ITOF is currently the only training program in the DoD which requires service members to earn certifications while attending "A" school as part of the curriculum and graduation requirements.

"I had no idea what I was getting into," ITSA James Takeda, of Gardena, CA, said. "I'm just thankful to be given the chance to do this. I had no background in computers at all, and now I am amazed at some of the stuff I know how to do."

The pilot phase of ITOF became the main IT course at CID in January, with 200 more students in training.

Sixteen current graduates are slated to begin "C" school at CID Corry Station in the new year leading the

future of ITOF into its next phase.

With the second generation coming aboard, current ITOF graduates are expected to help shipmates in the same fashion they were taught, making teamwork the staple of success.

IT "A" school Senior Enlisted Advisor ITC Jason Wiland emphasized that teamwork is critical to both individual success and the success of the new ITOF program.

"One of the first things I brief new students on is that there are others who have gone through this program before," Wiland said. "It takes a lot of discipline and dedication in and out of the class to get through this. These (newly-graduated) students now have the chance to be mentors."

Wiland instructed ITOF for the first five weeks of training, guiding students through their A+ certification, raising the bar for the weeks to come.

"The instructors could be hard and demanding, but it pushed us to do better," ITSN Zeerina Josan said. "If you want it bad enough, you will get it, and we wanted it. Looking back, I appreciated how we learned our stuff because I can remember things based on how they were taught."

Along with Wiland and Dise were a team of instructors, civilian and military, who taught specific lessons based on their area of expertise. Experience, 'sea stories' and on the job training complemented technical nomenclature and procedures, providing much needed context, painting a picture of just what an IT might run into ashore or afloat.

"I feel like I am prepared for anything now," Takeda said. "I'm expected to get 100 percent right, and I will do it." ✂

CID Receives Go-ahead for EIDWS Pin

Story & photo by Gary Nichols, CID Public Affairs Officer

PENSACOLA, FL – The Center for Information Dominance (CID) has become the first non-operational shore command to be approved for the Navy's newly created Enlisted Information Dominance Warfare Specialty (EIDWS) pin.

The EIDWS, along with the Information Dominance Corps (IDC) warfare pin for officers, are the first new pins to be approved for the Navy since it rolled out the Expeditionary Warfare Specialty pin in 2006.

The new warfare designation is an integral part of the IDC which was established Jan. 29, 2010, as part of the reactivation of the 10th Fleet at Fort Meade, MD.

In a speech to the Center for

Strategic and International Studies in October 2009, Chief of Naval Operations ADM Gary Roughead announced the future of cyber warfare. In addition to the 10th Fleet, he spoke about the creation of the Navy's newest corps as one of the centerpieces of that new cyber future.

"Right now we have a lot of ratings, a lot of specialties within the Navy that in and of themselves are a bunch of different communities, a bunch of different structures if you will," Roughead said. "And we will combine them into an Information Dominance Corps."

In this new corps, he said, the diverse communities would include Information Systems Technicians,

Cryptographic Technicians, Aerographers Mates, Information Professionals and Intelligence, and they would have a new warfare pin to reflect their new responsibilities.

"So what we have done is to take our already very proficient and experienced operators and create with them and with others an 'Information Dominance Corps,'" Roughead said.

"They will all be combined into an Information Dominance Corps, and when you add that together, it will constitute about 44,000 Sailors in the United States Navy. They will retain their individual identities, but they will be managed as a corps, they will

... continued on Page 32

(Far left) CID Commanding Officer Capt. Gary Edwards gives a pre-graduation pep talk to 20 students from the ITOF course pilot class at the CID headquarters building on board Corry Station. (Photo by Gary Nichols)



Information Dominance Requires Superior IT Service Management

By CDR David Wirth, Current Global Network Operations Officer, NETWARCOM

The Navy network is the largest interconnected network of computers operating under a single authority in the world. The Navy and Marine Corps Intranet (NMCI) has more than 390,000 user workstations, tens of thousands of servers, and countless network devices. With the addition of afloat networks, OCONUS Navy Enterprise Network (ONE-NET) overseas, Excepted Networks such as The Bureau of Medicine (BUMED), plus the remaining legacy networks, the Navy domain consists of more than a half million workstations and servers interconnected by government and commercial fiber, serving nearly one million users worldwide. Its sheer size and complexity is staggering.

Network operators tend to focus on the network because it is tangible.

It is what we manage. But the network and all its software and hardware are simply the tools used to deliver services. By themselves, they have no value. In the Navy, like in the best run civilian Information Technology (IT) operations, Information Technology Service Management (ITSM) focuses on delivering IT services to commands that are solely interested in the value those services provide in enabling their mission without forcing them to also own the costs and risks. Commanders and business users at sea and ashore care about their email and messaging, web services, Command and Control (C2), and logistics applications. They do not want to own the details, costs and risks of operating the enabling infrastructure; nor should they.

Recently, an IBM executive remarked to senior Navy leadership, "A network that is instrumented and interconnected enables intelligence." What the IBM executive left out was the importance of people and processes. A network that is instrumented and interconnected really only gives you data. Only people have intelligence. Without a consistent set of repeatable processes, one cannot turn data into actions that make the network appear intelligent and ensure stable and predictable availability for the warfighter.

The Information Technology

"... an average of 80 percent of mission-critical application service downtime is directly caused by people or process failures. Enterprises must also mitigate downtime risks caused by people and process failures. For these causes of downtime, strong IT operations and applications development processes are required."

Donna Scott
July 2001 Gartner publication

Infrastructure Library (ITIL) is a set of concepts and best practices for IT Service Management. Often described as 'common sense, documented,' ITIL is a set of industry best practices that provides a framework for building the structured, disciplined processes and functions needed to effectively define an overarching IT service strategy, design and test IT services, transition those services into the operating environment, and then operate them.

Unfortunately, like so many things that are common sense, the sense is only common after it's been defined. This article will focus on some of the ways Naval Network Warfare Command (NETWARCOM), operating on behalf of Fleet Cyber Command, works with its peers, subordinates and contractors to

operate, command and control the world's largest intranet using processes and functions built over an ITIL framework.

When NETWARCOM spun off its Manpower, Training and Equipping functions to Navy Cyber Forces (CYBERFOR) in January 2010, it put a singular focus on what ITIL calls IT Service Operation. The purpose of IT Service Operation is "to coordinate and carry out the activities and processes required to deliver and manage IT services at agreed levels to business users"¹ and warfighters.

The primary goal of Service Operation is to ensure stable

systems and consistent, reliable delivery of IT services. Of equal importance is the imperative of being responsive to the ever-changing requirements of customers and adversaries alike.

These competing priorities represent a polarity that requires constant attention to balance. The ability to be responsive to changing requirements while maintaining the availability of the network relies on the disciplined application of a set of repeatable processes to direct and manage available resources or reallocate them to specific missions, while maintaining stability throughout the change. According to NETWARCOM's Network Operations (NETOPS) Strategy, "The ability to exert control over these resources enables command functions, which is the ability to direct changes to resources as necessary to achieve a desired result within a specified timeframe."²

Maintaining reliable service availability also depends on knowing the status of the infrastructure and

detecting any deviation from normal or expected parameters; following established processes to preempt or prevent service interruptions; and restoring them as quickly as possible if they do fail.

One of the ways IT Service Management organizations ensure the stability and consistency of IT Services is through an Event Management process with control loops. ITIL defines an Event as "any detectable occurrence that has significance to the management of the IT infrastructure or service delivery."³ The control loop is a defined process where a single activity is monitored and compared against a predefined norm, or standard, to determine whether it is within an acceptable range of performance or quality. If not, a controlling action is taken to rectify the situation or to restore normal performance or service delivery.

Event Management is the core process that enables control. If we are monitoring the transport service, such as a satellite circuit, and are measuring bandwidth utilization on that circuit, the control loop compares actual utilization to the standard and trends over time. Comparing the trend to what is normal for that circuit at that time provides an opportunity to take controlling action if the service volume is trending in an unexpected direction to preempt an incident before it occurs. The NETOPS Commander can choose to increase capacity, reroute traffic, or filter lower priority traffic on that circuit in an effort to meet the war fighter's prioritized requirements on the mission critical services.

Occasionally, an event becomes an incident, which is defined as an "unplanned interruption to an IT service or reduction in quality of an IT service."⁴ Incident Management's primary objective is to restore normal service operation as quickly as possible and to minimize the disruption to operations.

Closely related to Incident Management is Problem Management. A Problem is defined in ITIL as the "unknown cause of one or more Incidents."⁵ Where Incident Management's sole objective is to

restore service as quickly as possible, Problem Management involves root cause analysis to determine and resolve the cause of incidents, prevent problems and resulting incidents from happening, eliminate recurring incidents, and minimize the impact of incidents that cannot be prevented.

Of the five processes defined in ITIL's *Service Operation* book (Event Management, Incident Management, Problem Management, Request Fulfillment and Access Management), Problem Management has the greatest and most obvious return on investment.

As alluded to earlier, Service Operation is but one of the IT Service Management Life Cycles defined in ITIL Version 3. While NETWARCOM and its subordinate NETOPS commands are primarily focused on Service Operation, there are a number of other ITIL functions and

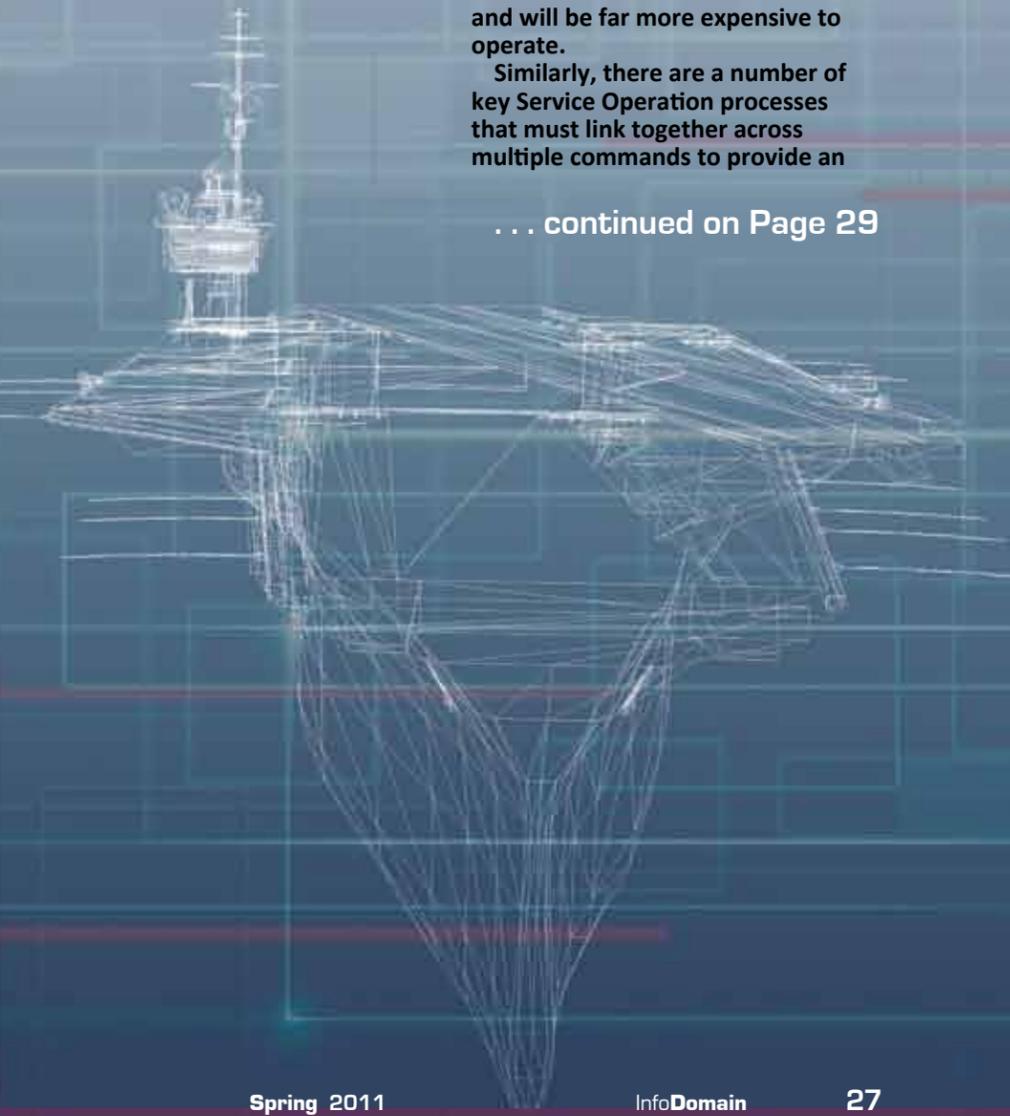
processes where NETWARCOM and its subordinates are heavily invested.

Change Management, Configuration Management, and Release and Deployment Management, for example, are primarily covered in the Service Transition publication and are largely owned by CYBERFOR and the various program offices. However, Service Operation commands submit requests for change (like new software, servers, etc.), deploy the changes, and maintain configurations.

Service Design activities are largely carried out by the Systems Commands (SPAWAR, NAVAIR, NAVSEA, etc). However, without significant participation of Service Operation staffs in all phases of design and testing, it is virtually certain that new services will not live up to expectations when transitioned to the live environment and will be far more expensive to operate.

Similarly, there are a number of key Service Operation processes that must link together across multiple commands to provide an

... continued on Page 29



VIRTUAL DESKTOP

Environment Helps Transform Training at FITC San Diego

By LT Wil D. Whiteman, Fleet Intelligence Training Center San Diego Public Affairs

SAN DIEGO -- Students from the International Maritime Intelligence Course who graduated Dec. 17 are among the first to benefit from the Virtual Desktop Environment (VDE) at Fleet Intelligence Training Center (FITC) San Diego.

FITC adopted VDE into its training suite, dramatically increasing the efficiency and adaptability of training systems while significantly lowering Information Technology (IT) support costs. The virtual environment takes advantage of network workstation PCs without hard drives, thus reducing the requirement for repetitive Information Assurance (IA) patches, updates and security measures on each individual computer. Using existing servers and workstations, FITC was able to implement VDE without any additional hardware costs.

"The conversion to 100 percent VDE was completed in October and its impact at FITC has been dramatic and quantifiable," said Frank Watson, FITC information officer.

"The Information Assurance return on investment for each patch, update or workstation security measure improved by a ratio of 26 to 1 over the previous system and also increased security, improved Local Area Network integrity, and mitigated risk," emphasized Watson. "The move to VDE also reduces the power consumption by 10 to 20 percent per workstation, resulting in a cost avoidance of approximately \$25 per year for each client station or more than \$10,000 annually for the command. With the

additional 50 percent reduction in computer lifecycle renewal costs by changing from expensive desktop PCs to virtual 'thin client' desktops that serve the same function, the impact on electronic classroom management processes and costs is significant."

FITC's VDE also provides enhanced remote access capability that was unavailable in the previous system. External training partners, commands and deploying platforms now have the capability to reach into the secure FITC schoolhouse training network using the NMCI-supported Citrix-access client to train on complex software suites and in FITC's existing scenario-based training environment. These suites were previously unavailable to the fleet without degrading their operational workstation capabilities or affecting workstation mission functions. The FITC VDE construct also enables adaptable training solutions for geographically-dispersed intelligence team members.

"Allowing the fleet remote access to our training network is a game-changer as they ready for deployment," said CAPT Mark M. Jarek, FITC commanding officer. "VDE also assists with the integration of our Information Dominance Corps partners around the globe."

"The large reduction in man-hours expended on information assurance allows my IT staff to focus on the needs of the instructors and students in and outside the schoolhouse," added Jarek. "The fact that VDE results in significant reductions in lifecycle renewal costs and energy consumption is an added

bonus for the command. Overall costs for the VDE project were substantially below the previous legacy IT infrastructure."

The September 2010 USS Ronald Reagan Strike Group Combined Cryptologic Intelligence Team Trainer was the first to employ VDE, enabling remote access with the Center for Information Dominance Learning Site, San Diego. In November, FITC integrated the USS Carl Vinson Strike Group Oceanographic Team into the Combined Cryptologic Intelligence Team Trainer while they conducted their final meteorology certifications.

FITC staff and students alike have been exceptionally pleased with the impact VDE is having at the command. "Deploying FITC's thin client solution, VDE, has been transformational," said Watson. "As critical information assurance updates are released, we can now react efficiently, guarantee patch deployment results quickly, and get right back to enabling the best support to training possible, supporting the fleet Sailors today and in the future even more efficiently than we have in the past."

For more information about the Fleet Intelligence Training Center, San Diego visit: <https://www.netc.navy.mil/centers/cennavintel/fitc/>.

For more information about the Naval Education and Training Command visit the NETC website at: <https://www.netc.navy.mil/>.

Graphic Illustration by Robin D. Hicks



IDC



VDE



IA



NETWORK
PC



LEGACY
IT



FITC
SAN DIEGO

effective IT support structure. Problem Management, in particular, requires close cross command collaboration for conducting the root cause analysis behind incidents. This process is critical for making the programmatic and resource decisions necessary to effect changes in the infrastructure, manning, training, and control processes to prevent problems from recurring and to minimize the impact of incidents that cannot be prevented.

In a July 2001 Gartner publication, Donna Scott wrote, "According to Gartner research, an average of 80 percent of mission-critical application service downtime is directly caused by people or process failures."⁶ She goes on to explain that most enterprises tend to invest in adding redundancy to the network in an effort to increase reliability. While that is important, according to Scott, it cannot and should not be the only line of defense. "Enterprises must also mitigate downtime risks caused by people and process failures. For these causes of downtime, strong IT operations and applications development processes are required."⁷

Eighty percent! We have a lot of work to do and the world is not waiting. If information is to be the game changer; if our dominance in its use is to be the force multiplier our Navy demands; then our Navy must have the ability to reliably manage the services that deliver it. ITIL provides the structured framework over which to build the processes and functions needed to deliver the IT services the Navy relies on to fight and win.

For deeper understanding, a full set of ITIL courses, from "Cultural Awareness" through "ITIL Expert" is available online for members of the Information Dominance Corps and all designated IA Workforce members at SkillPort <http://navyiacertprep.skillport.com>.

- 1 Office of Government Commerce. *Service Operation*. (Great Britain: The Stationery Office 2007)
- 2 NETWARCOM. *Strategy for Network Command and Control*. (Norfolk, VA: U.S. Navy 2009)
- 3 Office of Government Commerce. *Service Operation*. (Great Britain: The Stationery Office 2007)
- 4 Ibid.
- 5 Ibid.
- 6 Scott, Donna. "NSM: Often the Weakest Link in Business Availability." Gartner. 3 July 2001. (ID Number: AV-13-9472)
- 7 Ibid.

NEIRP Supports Navy Commands Requiring Unpriced IT Services

By Jacky Fisher, NGEN PAO and the FITT Team

The Navy Marine Corps Intranet (NMCI) Continuity of Services Contract (CoSC) for information technology (IT) network services was awarded to Hewlett Packard-Enterprise Services (HP-ES) in July 2010 and has been in effect since October.

NMCI CoSC established the requirement for government command and control (C2) over NMCI service and infrastructure. NMCI CoSC is a transitional state that allows the foundations to be built for the Next Generation Enterprise Network (NGEN); a step to achieve the net-centric capabilities specified in the Department of the Navy's Naval Networking Environment (NNE) Strategy. The goal for the future is not to change the way the end user functions in the network environment, but rather to alter how elements supporting the network environment are managed.

With these network environment changes, revising the approval and validation process for IT service requests became necessary. Under NMCI CoSC, the Contract Line Item Number (CLIN) ordering structure and funding streams were adjusted to separate out the fixed costs (routers, switches – 'behind the wall plug') and the variable costs (desktops, monitors – 'in front of the wall plug'). Echelon II commands are responsible for their seat 'variable' costs, while the enterprise budget (i.e. fixed costs) is managed separately. With this shift in business practice, a process for managing unpriced IT service requests and their effect on the overall technical baseline became apparent.

In late December 2010, Commander, Navy Cyber Forces (CYBERFOR) announced the development of the Navy Enterprise IT Requirements Process (NEIRP). The NEIRP is based on existing NMCI CoSC process best practices, and is in accordance with the OPNAV N2/N6 resource management policy. The design of the NEIRP guide is nearing completion, with CYBERFOR the final approval authority. See "Roles & Responsibility" on top of next page for a summary of NEIRP stakeholders.

"During NMCI, Echelon II commands could purchase whatever they required, with no real consideration or planning for what effect these purchases had

on the overall technical baseline and cost to the Navy enterprise," said Eric Markland, NNE Division Head and Director, NGEN Fleet Implementation and Transition Team (FITT). "The Navy Enterprise IT Requirements Process will change this paradigm by setting the governance to ensure requirements are reviewed and validated against enterprise objectives, and to ensure the baseline is properly maintained, managed and resourced."

This process is expected to be deployed as a pilot program to selected Echelon II commands mid-February 2011. This approach will enable process and training refinements to be observed through lessons learned prior to full deployment, which is planned for the April 2011 timeframe.

"Input from stakeholders has been essential in developing this process," Markland said. "We're not looking for this process to be a CYBERFOR mandate. With stakeholder inputs, we'll learn better how to prioritize and manage requests in order to more efficiently and effectively develop solutions for the end users while ensuring enterprise objectives are met."

Designed to safeguard against duplicate spending, obtain visibility on IT expenditures and capture lifecycle costs, the NEIRP will support Navy commands requiring unpriced IT services under NMCI CoSC. Each unpriced requirement will be reviewed and validated for solution designs that are technically sound, cost effective and supported by the enterprise. Impact to the enterprise with reference to technical baseline and total cost of acquisition and sustainment remains a major objective of the validation process.

The functionality and goals of the NEIRP have far-reaching capabilities as the Navy continues the move from NMCI CoSC to NGEN. "As we move towards process deployment," states Markland, "I'm confident that the NEIRP will achieve its intended objective of creating the necessary structure and governance critical in ensuring Navy IT requirements are validated and managed in order to better provide enterprise solutions under NMCI CoSC and in the future, NGEN." ✂

Roles & Responsibility

The NEIRP will be supported by several organizations due to the complexity of the review and analysis required to effectively validate, approve and fund each requirement and supporting solution.

- Chief of Naval Operations (OPNAV N2/N6)
- U.S. Fleet Cyber Command and U.S. Tenth Fleet
- PEO-EIS
- Echelon II CIO
- Navy Cyber Forces N8 (Requirements)
- Navy Cyber Forces N1 (Manpower)
- Naval Network Warfare Command Office of Designated Approval Authority (NETWARCOM ODAA)
- Space and Naval Warfare Center (SPAWAR)
- Budget Submitting Offices (BSO)
- Vendor(s)

NMCI Program Manager Receives Excellence Award

By Denise Deon, NMCI Public Affairs Officer

SAN DIEGO - The Navy Marine Corps Intranet (NMCI) Program Office is pleased to announce that CAPT Scott N. Weller, USN, NMCI program manager, is a recipient of a Department of the Navy (DON) Information Management (IM) Information Technology (IT) Excellence Award.

Weller received the award for advancing NMCI while ensuring the network continued without interruption as it transitioned to the NMCI Continuity of Services Contract (CoSC). He accepted the award Jan. 25 at an awards ceremony held at the San Diego Convention Center.

The DON IM/IT Excellence Award is given to individuals and programs with outstanding contributions toward transforming the Navy and Marine Corps through information technology. The annual award was presented to Weller by Terry Halvorsen, the DON Chief Information Officer (CIO).

"Receiving the DON IM/IT Excellence Award is truly an honor," said Weller. "It is gratifying to

know that my contributions are recognized by DON CIO in impacting, transforming and advancing Naval IT. It has been an honor and a privilege to lead NMCI, an IT network that is invaluable in providing the day-

to-day business operations and ensuring that mission critical needs are met for the warfighters."

Weller is responsible for the management of NMCI, the largest and most secure enterprise-wide



(Left to right) CAPT Scott Weller poses with Janice Haith, Director Assessments and Compliance; Mr. Terry Halvorsen, DON CIO and Marine Col. Jim Dillion, Head, Network Plans & Policy Division, after being awarded the DON Information Management (IM) Information Technology (IT) Excellence Award at the AFCEA West 2011 conference in San Diego. (Photo by Greg Vojtko)

Graphic Illustration by MC2(SW) Joshua J. Wahl

... continued on Page 42

develop as a corps and they will fight as a corps.”

Since its inception in 2005 CID has led the fight by using a multi-disciplinary, asymmetric approach to training joint warfighters for cyberspace and to dominate the information domain.

CID CMC(SW/AW) Christopher Thompson explained that it makes sense for CID to be selected for the EIDWS because CID develops IDC Sailors.

“Our command is named Center for Information Dominance,” Thompson said. “So when the Navy implements a new warfare program, named Enlisted Information Dominance Warfare Specialist, one would think CID would be the leader for this warfare program because we train virtually every aspect of the EIDWS program. Minus the meteorology and the intelligence portion, CID teaches everything within the Information Dominance Corps.”

Ironically, as a shore-based training command, CID wasn’t one of the commands initially selected to be an authorizing authority for the EIDWS.

In October 2010 CID Commanding Officer CAPT Gary Edwards selected Senior Enlisted Advisor CTRC(SW/AW) Doc Wallach to form a team of subject matter experts (SME) from CID to come up with an EIDWS qualification program for CID instructors.

Over the next several months Wallach and his group of 23 active duty and retired chief petty officers – all experts in their respective fields – labored during weekends and off-duty hours to develop a qualification program so CID instructors could have the chance of qualifying for the EIDWS.

Wallach said putting together the entire program from start to finish was especially challenging since none of that work was done during duty hours. The reason, he said, is because CID’s primary mission of training Sailors and joint service members is too important to compromise by working on extra-curricular work, even for important work such as the EIDWS program.

He said the experience was invaluable because each member of his team learned a lot about their

individual rates along with the rates of their fellow cryptologists and information systems technicians.

When CID’s qualification program was finally completed to the satisfaction of Thomson and Wallach’s team, they invited Navy Cyber Forces Force Master Chief (AW/SW) Jay Powers, to Corry Station, the home of CID, to evaluate their new program.

Thompson, Wallach and CID’s team of SMEs were a little nervous about the visit because the original instruction was written for operational commands.

“He (Powers) was skeptical about a training command – a non-operational command – being approved for the program,” Thompson said. “So he came down here thinking that he probably would not approve the program and he told us this ahead of time.”

Following the evaluation, Powers told the working group they had developed a solid, well-thought out and thorough qualification program, probably the best he had seen to date. Nevertheless, they would learn what his decision would be at the end of the day.

“The only thing that was going through my mind was that I might have to face all these SME who had put all these months of effort into this project and tell them ‘I’m sorry that I wasted your time,’” Wallach said. “That’s what I was most fearful of.”

During an all-chiefs meeting at the Chiefs Mess on board Corry Station at the end of the day, the team finally had the answer they were hoping for.

“CID is the birth place for our IDC Sailors,” Powers said. “CID’s entrance into the Enlisted Information Dominance Warfare program brings a wealth of battle-tested experience and continues the development and qualification of our Navy Master Training Specialist (MTS) IDC Sailors. As I reviewed your program it became crystal-clear to me that not only does the EIDWS program belong here, but it promises to be the gold standard for all other EIDWS programs across the globe.”

Each CID instructor is currently mandated to earn their MTS. Now they will be required to earn their

EIDWS before completing their tour of duty at CID.

Wallach said shore duty at CID is going to be even more rugged now due to the rigorous EIDWS qualification process, but the instructors will become better Sailors because of the new requirements.

CID Executive Officer, CDR Michael Douglas, said he was proud of the monumental effort by his chief petty officers who put the successful EIDWS qualification program together.

“These Chiefs really exemplify the concept of one team, one fight,” Douglas said. “This new warfare qualification pin shows the world that CID Sailors are leading the effort to protect and defend the information domain, and I believe they really deserve this recognition for their contribution.”

“They are going to be the best of the best in the community and probably the future leaders in the community,” Wallach said.

The group of SMEs at CID Corry Station are scheduled to take their qualifying examination the first week of March. If and when they qualify and their program is certified by Powers, every CID instructor throughout the CID domain will be eligible to qualify for – and if successful – proudly wear the new EIDWS pin.

“We’re going to challenge them every step of the way,” Thompson said. “In essence what we’re doing is taking a great Sailor and making them even better. When they complete their tour here at CID, they’ll be a better, more well-rounded Sailor, and any command will be fortunate to have one of our instructors join their ranks.”

CID is the Navy’s Learning Center that leads, manages and delivers Navy and joint force training in information operations, information technology and cryptology.

With a staff of more than 1,050 military, civilian and contracted staff members, CID Corry Station oversees the development and administration of more than 168 courses at 16 learning sites throughout the United States and in Japan. CID Corry Station provides training for more than 19,000 members of the U.S. Armed Services and allied forces each year. ✎



Navy's NGEN Tactical Afloat Network Presses Forward

By Steven A. Davis, SPAWAR Public Affairs

SAN DIEGO – The Consolidated Afloat Networks and Enterprise Services (CANES) program met key cost, schedule and performance entry criteria and received a Milestone B Acquisition Decision Memorandum Jan. 10.

The approval was based on the program’s ability to meet key defense acquisition efficiency criteria such as maximizing competition, streamlining the acquisition process, targeting affordability and controlling cost growth.

CANES is the consolidation and enhancement of five shipboard legacy network programs and will provide the common computing environment infrastructure for command, control, communications, computers and intelligence (C4I) applications that currently require system specific infrastructure to operate legacy systems.

“This is an extremely significant acquisition milestone for the CANES program as it validates technology maturity, stable requirements and a fully funded program,” said CAPT D.J. LeGoff, program manager for the Tactical Networks Program Office. “Our next step in the acquisition process is to take the proper programmatic steps to demonstrate the ability of CANES in an operational environment.”

Milestone B is the initiation point for acquisition programs and official entry into the Engineering and Manufacturing Development phase of a program’s lifecycle. The purpose of this phase is to develop a system, complete full system integration, develop an affordable and executable manufacturing process, and demonstrate system integration, interoperability, safety and utility.

The Milestone B decision, which also included Milestone C entrance criteria, allows for the production of four limited fielding units. These units are intended for operational and training use and will not be installed until completion of an operational assessment and a successful Milestone C decision. At this point the program will enter the Production and Deployment phase.

The Navy’s Program Executive Office for C4I oversees the CANES program and is managing competitive system development contracts with Lockheed Martin and Northrop Grumman.

The CANES program is at the forefront of recent acquisition reform changes directed by the Undersecretary of Defense for Acquisition, Technology and Logistics (USD AT&L). A recent series of ‘Better Buying Power’ memorandums directed Defense Department acquisition organizations to pursue initiatives in the following five areas: (1) Target Affordability and Control Cost Growth (2)

Incentivize Productivity and Innovation in Industry (3) Promote Real Competition (4) Improve Tradecraft in Services Acquisition and (5) Reduce Non-Productive Processes and Bureaucracy.

“CANES meets the spirit and intent of what the Department of Defense wants acquisition programs to be doing to obtain greater efficiency and productivity in defense spending,” explained LeGoff. “In alignment with USD AT&L’s acquisition roadmap, the program foundation is built upon cost containment, open architecture and competition throughout the program’s lifecycle.”

Consolidation through CANES will eliminate many legacy stand-alone networks while providing an adaptable and responsive information technology platform to rapidly meet changing warfighter needs. This strategy strengthens the network’s infrastructure, improves security, reduces the existing hardware footprint and decreases total ownership costs.

In addition to providing greater capability, CANES will allow fleet end-users to benefit from reduced operations and sustainment workloads as a result of common equipment, training and logistics.

CANES introduction to the fleet will begin with installs in 2012 on unit level ships with two Engineering Development Model installations, followed by Limited Deployment installations in 2012 that cover force level ships, shore sites and additional unit level ships. CANES will be deployed to more than 190 ships, submarines and Maritime Operations Centers by 2021. ✎

Office of the Secretary of Defense Cost Assessment and Program Evaluation/CANES Assessment

- Financial return on investment to the Navy for CANES implementation is 8.1 percent.
- Benefits will meet requirements by increasing operational capability, performance, situational awareness and security to the Navy.

Graphic Illustration by Robin D. Hicks

IO Range Provides Key Internet Service And More

By Jacky Fisher, CYBERFOR Public Affairs

Making clouds and creating time. Theology? No. The government. And yes, they are here to help. The Joint Information Operations (IO) Range, sponsored by the Office of the Undersecretary of Defense (Intelligence) and supported by the United States Joint Forces Command (JFCOM) Information Operations (IO) Joint Management Office (JMO) in Norfolk, Va., makes clouds, creates time and is aggressive in its mission to keep United States Department of Defense (DoD) safe from cyber attacks.

The Joint IO Range is designed to create flexible, seamless and persistent environments enabling combatant and component commanders to have the same level of expertise in employing IO

weapons as they have in employing kinetic weapons. Within the Joint IO Range enterprise, IO technologies and tactics are assessed, tested and exercised. The end result is identifying joint training and experimentation requirements, as well as developing technical solutions for warfighters.

That's the PowerPoint definition of the IO Range.

Army Lt. Col. John Ballard, chief of the Joint IO Range, explains it like this, "If someone did not have an idea of what an IO range is, I would say simply that we are a classified Internet service provider. When you go to Google, you're going to a server somewhere that provides a capability -- the backbone from which you got there is completely invisible to you. That's what we

do for the warfighter. We provide them that backbone, that pipe, and the expertise, targets and relationships needed to leverage information-related capabilities inside that environment."

To understand the mission and national security importance of the Joint IO Range, IO must first be understood. The new doctrinal definition of IO emphasizes the integrated employment of information-related capabilities and de-emphasizes the current definition's reliance on the five core capabilities: Computer

"If someone did not have an idea of what an IO range is, I would say simply that we are a classified internet service provider. When you go to Google, you're going to a server somewhere that provides a capability -- the backbone from which you got there is completely invisible to you. That's what we do for the warfighter. We provide them that backbone."

**Army Lt.Col. John Ballard
Chief of the Joint IO Range**

Network Operations (CNO), Electronic Warfare (EW), Military Deception (MILDEC), Operations Security (OPSEC) and Military Information Support to Operations (MISO, formerly known as PSYOP) (see graph 1 for definitions).

Exercising some or all of these core capabilities in a 'cyber range' environment -- a secure closed-loop network that supports developing, experimenting, testing, training, integrating and synchronizing these core capabilities, with persistent and emerging IO and cyber activities -- this is what the Joint IO Range does.

In 2003, the Undersecretaries of Defense for Intelligence and for Acquisition, Technology and Logistics joined with the Director

of Operational Test and Evaluation and challenged JFCOM "to see if this thing called the IO Range is technically possible and what it would cost to interconnect (already existing) capabilities," according to Chuck Campbell, department chief of the IO Range. The IO range was to be an environment to test IO capabilities, focused primarily on CNO and EW.

In 2005, then Deputy Secretary of Defense Gordon England designated JFCOM as lead agent (LA) for the Joint IO Range. The following year, the Initial Operating

Capability (IOC) stood at 10 nodes (associated hardware and connections used to run an exercise that can be either fixed or portable) and three use cases. In 2010, those numbers jumped to 68 nodes and 65 events. (Currently,

the number of nodes is nearing 70, counting the deployable ones. But not all of them are in the network at the same time).

Joint IO Range events can employ up to a dozen or more virtual private networks; that's how complex these scenarios have evolved in just four years. The demand for Joint IO Range support continues to increase at an exponential rate. "Activities in the cyber domain will continue to develop and our warfighters must maintain the upper hand by leveraging information related capabilities for offensive and defensive military operations," Campbell said. "The Joint IO Range is where those warfighters come to access and employ those capabilities." ☺

EDITOR'S NOTE: In the next edition of InfoDOMAIN, find out how the Joint IO Range get its authorities by using cryptologically isolated virtual private networks, how time and clouds are created, and how this increasingly important capability is being used to strengthen U.S. cyber security.

For more information on how your command can use the Joint IO Range, contact the JIOR requirements lead Dave Blake, Joint IO Range Requirements, at IOR-Regs@jfc.com, (757) 836-9651. Reserve Units or Reserve personnel with security clearances wanting to drill at one of the Joint IO Range sites may contact Chuck Campbell, chuck.campbell@jfc.com, (757) 836-9948.



IO Capabilities

Operations Security (OPSEC)

- Slows adversary's decision cycle; enabling friendly forces to attain objectives.
- Denies adversary critical information about friendly forces' capabilities.
- Early integration into mission planning is essential to reducing indicators of impending operations.

Military Information Support to Operations (MISO)

- Actions taken to convey selected information/indicators based on the truth to foreign audiences to influence emotions, motives, reasoning & behavior.

Military Deception (MILDEC)

- Effects adversary intelligence collection, analysis & dissemination systems.
- Focused on affecting a desired behavior, not just confusing the intended recipient.
- Cause adversary commanders to form inaccurate impressions & take desired actions.

Electronic Warfare (EW) – subdivisions: Electronic Attack (EA), Electronic Protection (EP) & Electronic Warfare Support (ES)

- EA: degrade, neutralize or destroy adversary's effective use of the electromagnetic spectrum.
- EP: minimizes adversary EA, involves actions such as self-protection jamming & emission control, & using technology to limit effects.
- ES: collection used to produce signal intelligence (SIGINT), both communications (COMINT) and electronic (ELINT)

Computer Network Operations (CNO) – Comprised of Computer Network Attack (CNA) & Computer Network Defense (CND)

- CNA: Operations to disrupt, deny, degrade or destroy information resident in computers & computer networks.
- CND: Defend against CNA.

Public Key Infrastructure:

Coming to a SIPRNET Computer Near You

By Seth Gang, NETWARCOM CIO IA

Accessing your Secret Internet Protocol Router Network (SIPRNet) account is about to get easier and more secure. Accounts on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) have required the use of Public Key Infrastructure (PKI) certificates on a hardware token, such as the Common Access Card (CAC), for several years. Similar security mechanisms are now being deployed to the SIPRNet.

What does this mean for you as a SIPRNet user? You will no longer have to remember a long, complex, ever-changing password to access your account. As this capability is deployed across the Department of Defense (DoD), SIPRNet websites will also transition away from passwords and will require PKI-based authentication.

SIPRNet PKI has been around for many years, but was only available in software certificate form. The DoD PKI Program Management Office (PMO), an office jointly run by the Defense Information Systems Agency (DISA) and the National Security Agency (NSA), identified a hardware token solution for SIPRNet PKI.

Your CAC is not authorized for use on any classified networks due to security requirements, but the SIPRNet solution uses technology similar to the CAC to place PKI certificates on a smartcard. The SIPRNet smartcard itself is unclassified when removed from the SIPRNet workstation, which means it requires no more protection or special handling than the CAC; the card can be locked in a desk drawer or kept in your wallet.

In 2010, a small pilot test of the hardware token based SIPRNet PKI was conducted on the Navy Marine Corp Intranet (NMCI). This pilot of 150 users successfully tested the ability to use Cryptographic Log-On (CLO) to the network, access Public Key (PK) enabled websites, digitally sign email, and encrypt email using the SIPRNet PKI hardware token.

The DoD PKI PMO is now ready to conduct an Initial Operational Test & Evaluation (IOT&E). This will include up to 50,000 SIPRNet users throughout the DoD, with about 10,000 Navy users from select commands in Hawaii, San Diego, the national capital region, and Norfolk/Virginia Beach. The evaluation will run this spring, and full deployment of SIPRNet PKI to all DoD users will begin as early as this summer. The USS Bonhomme Richard (LHD-6) will be the Navy's first ship to begin using SIPRNet PKI later this year.



All SIPRNet users can expect to receive their SIPRNet smartcards by the end of fiscal year 2013.

U.S. Cyber Command recently issued Coordination Alert Message (CAM) 11-004, SIPRNet PKI Implementation, Phase I with guidance on what efforts should be completed now. Commands should begin preparing now for the coming SIPRNet PKI requirements. Each command will be required to identify two SIPRNet PKI Trusted Agents to assist with issuing cards to their command.

The cards, readers and middleware will be centrally funded by DoD through fiscal year 2014, but network owners will be responsible for any other enablement costs. Further technical information, guidance, and frequently asked questions regarding the Navy's PKI program can be found on the NIPRNet at <https://infosec.nmci.navy.mil/PKI> or on the SIPRNet at <http://infosec.navy.smil.mil/PKI>.

EDITOR'S NOTE: Seth B. Gang is the Identity Protection & Management lead at Naval Network Warfare Command (NETWARCOM). Questions regarding SIPRNet PKI or other Information Assurance (IA) matters can be sent to NETWARCOM_LTLC_CIO_IA@navy.mil. You can also find other IA information on the NETWARCOM portal at <https://www.portal.navy.mil/netwarcom/CIO>.

Team Reaches Out to Community & Supports Month of the Military Child



By James Magdalenski, Director, Naval OPSEC Support Team

Who's Face is in Your Book? This theme is depicted in posters throughout the hallways of Cape Henry Collegiate School (CHCS), Virginia Beach, VA, as students in all grades focus on the significant impact social media has in our day-to-day activities and lives. Recently, staff and students have focused on the vulnerabilities associated with social networking.

So where better to turn in the Hampton Roads, Virginia, area when talking about the vulnerabilities of social networking and making our personal information public, than the Navy's Operations Security (OPSEC) Support Team (NOST) located at Navy Information Operations Command, Norfolk.

Working closely with Randy Pike, Director of Guidance, and a student committee, Lee Case from the NOST presented an OPSEC and Social Networking brief specifically tailored to high school students. The student committee "unanimously agreed the students and parents at Cape Henry needed

to hear this presentation because there was much they did not know," said Pike.

After presenting the brief to the senior class, one student summed it up by saying, "I think people, especially our age, really think to themselves, 'oh that's not gonna be me'. And they're oblivious to other people's perspectives. It is important because it's something that can be taken out of their control."

Case concentrated in a couple of areas where young people on the social networking highway can make themselves vulnerable. Understanding there is not true "delete" key on the internet, posting negative or derogatory comments, or lewd photos can come back and haunt you in the future, whether it be in a few months when applying to a college or five years when looking for employment. Colleges and places of employment will undoubtedly review your social networking site to see if you "fit" into their organization.

Another perspective is from an adversarial or 'bad guy' angle. Placing too much personal information on a site can leave not only you, but your family vulnerable to identity theft or home invasion when you post everyone is out of town on vacation. Seemingly harmless information can be a gold mine to people with other motives.

Pike also stated, "As adults we know how dangerous and vulnerable young people can be with all of these social networking sites. It is important to give them the education to understand this and they hear it better from a different voice. Lee Case is able to 'speak their language' and educate them in so many important ways."

In support of the 'Month of the Military Child' in April, the NOST presented similar briefs to military children in the Fleet and Family Support Center youth programs at Joint Expeditionary Base Little Creek and Naval Air Station Oceana. ✂

Graphic Illustration by MC2(SW) Joshua J. Wahl



San Antonio-Based Sailors, Marines Complete 223-Mile Non-Stop Relay Race

By CTIC(EIDW) Micah T. Epley

CORPUS CHRISTI, TX - A team of nine Sailors and Marines from National Security Agency/Central Security Service (NSA/CSS) San Antonio completed the country's longest non-stop relay race Oct. 15 and 16.

The 223-mile long race took place over a 34-hour period and was part of the inaugural 'Capitol 2 Coast' race from Austin to Corpus Christi.

Billed as the 'Great Texas Relay', each of the San Antonio-based servicemembers ran approximately 25 miles for their individual legs, with an average pace of about nine minutes per mile.

CTI3 Mark G. Wiggins explained the strategy behind accomplishing such a feat. "The fact that we each ran approximately the equivalent of a marathon might sound daunting, however as with most things in the military, we were able to use portions of our training."

"As Sailors, we are often tasked with seemingly impossible missions," explained Wiggins. "The only way to achieve success and finish these difficult tasks is through teamwork and by breaking the whole into smaller parts. Your only thought is to finish the next segment, or in this case, the next mile. By segmenting the task, the whole becomes much more manageable. Every time one of our guys finished a leg, his teammates were there to cheer on and to send the next poor soul off."

A couple of the members of the team had been logging considerable mileage in preparation for the race; however, most did not deviate from their normal workout routines. Several trained using Crossfit style, while others preferred to take a more casual approach to their preparation. Prior to the relay, one of the runners had never run farther than five miles in any one run.

CTRC(NAC) Michael Hernandez, Navy Information

Operations Command (NIOC) Texas Command Fitness Leader, was very impressed with the teamwork and accomplishment of the team.

"The performance of these Sailors is a true testament to our Navy's success in validating the importance of year round physical readiness," Hernandez said. "It also helps to dispel the old perception that the Navy's physical readiness program is only a bi-annual evolution. Simply put, Sailors are getting in shape and maintaining it year round through a bonafide culture of fitness."

The idea to compete in this inaugural relay race was born when CTI2(SS) Christopher M. Steinke was surfing the net in search of community running events. Seeing that the finish line for the Capitol 2 Coast relay was on the coast of Corpus Christi, in front of the USS Lexington, he knew there had to be a Navy presence. A couple of phone calls and emails later, the team was quickly formed.

In the cool morning air, while most of the citizens of Austin slept, and surrounded by hundreds of race enthusiasts and fellow service members, the NSA/CSS team started their long journey at the steps of the Capitol building in Austin. Once the team left the Austin city limits, they continued down farm roads and passed through the occasional town. Taking in the sites and scenic Hill Country, the team observed a magnificent Texas sunset as they completed the second leg in the city of Seguin.

Thirty-four hours later the entire team ran the last quarter mile as a team as CTI3 Ryan Miller officially crossed the finish line. They immediately jumped into the Gulf of Mexico to cool down celebrate their victory.

The team finished second in the 'Hero' division and ninth overall. ✂



(Left to Right) CTI3 Ryan Miller, CTI1(SW) Arturo Campbell, Marine Cpl. Thomas Grafe, CTI2(SS) Christopher Steinke, CTI3 Andres Albizo, CTI2 Charles Rose, CTI3 Stephen Hatchett, and CTI2(EXW) Anthony Petrillose. Not pictured is CTI3 Mark Wiggins. (Photo by Haley Willoughby)



Official U.S. Navy Photo

(Left to Right) Phil Cultrera, Andrew McKenna, Penny Maker, David Burns, Mark Faulkner, Dave Green, Keith Labonte, Bruce Flood, Daniel Williams, and Jeffrey Stevens.

Voluntary Protection Program: A Safety Program You Can Live With

From NCTAMS LANT Det. Cutler Public Affairs

Since 2009, the Naval Network Warfare Command has been enrolled in the Occupational Safety and Health Administration (OSHA) Voluntary Protection Program (VPP) to support Naval Computer and Telecommunications Area Master Atlantic (NCTAMS LANT) Detachment Cutler located in Maine.

VPP is a premier OSHA safety program that has a proven record of improving safety, and reducing accidents, injuries and associated costs. Established in 1982, the initiative was developed to recognize and promote a more effective worksite based on a safety and health management system. Initially, 11 companies participated. In 2007, more than 1,800 companies and federal organizations were enrolled.

The foundation for the success of this program is employee involvement. VPP enhances workforce motivation and dedication to working safely at all times – at work and at home. The program allows supervisors and managers more free time to spend on the mission, reducing the need for

time and focus on safety problems, workplace injuries, lost time accidents, or equipment failures.

According to the National Safety Council, preventable injuries cost the Department of Defense (DoD) an estimated \$10 - 21 billion per year. VPP worksites help to reduce these costs, coming in at 52 percent below the industry average for Days Away, Restricted or Transferred (DART) cases, which measure employee absences due to accidents or injuries. In addition, VPP worksites have an associated reduction in Workers Compensation costs by an average of 20 percent per year, along with an overall program return on investment of more than 150 percent.

At Detachment Cutler, during the initial stages of implementing the program, the Technical Director, the Safety Manager, and the Safety Committee became concerned because there was an increase in safety issues rather than a reduction.

"We soon realized the issues being raised were not new, but had existed all along," said Sam Seavey,

Safety Manager, Detachment Cutler. "We were not aware of the issues because they were not being reported. This increase in safety reports was proof that enhanced employee involvement and motivation leads to improved safety awareness."

With the support and oversight of the Technical Director, the Safety Manager, and Union officials, the Safety Committee implemented several goals and objectives to meet the requirements of the VPP, and the results have been extremely successful. Some of the programs the committee established are:

Completion of Required Safety/VPP training - This program has been responsible for an improvement of employee safety training completion rate from approximately 75 percent to 97 percent.

Implementation of Work Area Self Inspection Program - Designed to enhance the involvement of the supervisors and employees. Each month supervisors

... continued on Page 40

select an employee to accompany them on safety inspections throughout facilities where they work.

Abatement of Hazards and OSH Deficiencies -There have been significant improvements within the command in getting safety deficiencies abated in a timely manner.

Increasing Near Miss Reports -Safety professionals say that, typically, a safety infraction or near miss will occur 1,000 times. Out of that, there will be a mishap about 100 times. The 100 mishaps usually result in 10 injuries and out of the 10 injuries there is usually one fatality. When the workforce is motivated and involved, once the incident is discovered and reported as it occurs, actions are taken to abate it, and that helps to prevent additional injuries from occurring.

VPP 'PASSPORT' Program -This is an incentive tool to enhance employee involvement. Each employee is encouraged to participate in this program on a voluntary basis. Designed to give employees a greater overview and perspective of a variety of safety issues they may not be accustomed to, employees are provided a pamphlet comprised of 45 safety related topics or actions. The employees are required to complete 10 mandatory items and 15 items of their own choosing. When the required number is achieved, the employees receive a \$200 on-the-spot cash award and an eight-hour time-off award.

Seavey is ecstatic with the success of the program citing, "Each and every day there are improvements to the program and positive results being achieved." Seavey had not

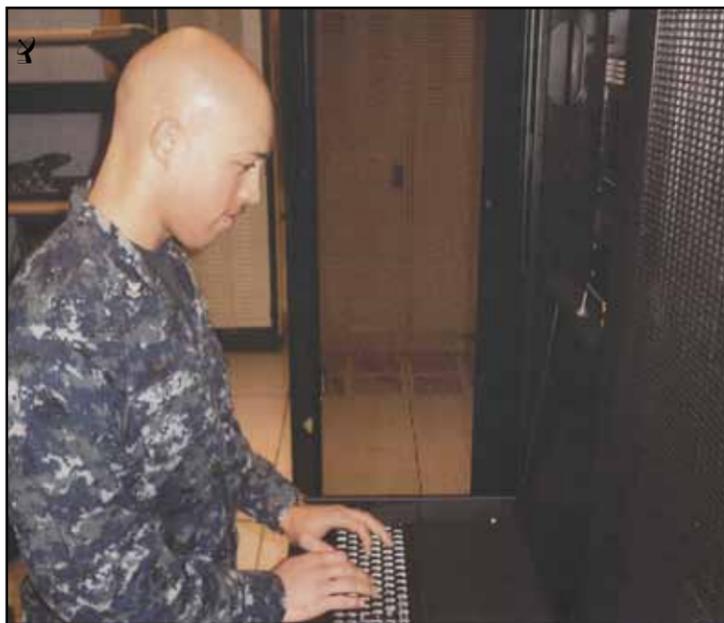
expected the turn-around to occur as fast as it has with only 10 months of activity in the program.

"The best is yet to come as we leave the preparatory stages and move forward into the full enactment phase," added Seavey. "Based on our initial accomplishments, the successes ahead are hard to even imagine."

The ultimate goal of the command is to achieve VPP STAR status, which can take up to two years. There are numerous challenges to enrollment in VPP and successful achievement of STAR status. Complete guidance and assistance for DOD agencies and facilities personnel is provided at website <http://vppcx.org/>. This site has a tremendous amount of information, insight and lessons learned from the experiences of those DOD affiliates that have been successful in achieving STAR status. ✎

Take Charge & Move Out: Vital Component of NCTS JAX's Mission

By ET2(SW) Tyler Kirkland, NCTS Jacksonville Public Affairs



ET2 Gregory Rouzeau double checks one of NCTS JAX's TACAMO-VBB systems to ensure operational readiness 24/7/365 days a year. (Photo by ET2(SW) Daniel Diedrich)

Imagine if everyone's worst nightmare were to come to fruition — a fierce enemy threatens nuclear war. Could America survive a first strike? Could our strategic communication nodes be eliminated, rendering us defenseless? Enter the nation's "Take Charge And Move Out" (TACAMO) system.

With the TACAMO system in place, the president and his top military officials maintain survivable communication links with the air, land and sea-based weapon delivery systems in the nation's arsenal. After a recent equipment installation, Naval Computer and Telecommunications Station, Jacksonville (NCTS JAX), now plays a large part in making sure this capability is operational at all times.

During 2010, NCTS JAX implemented the Hybrid-TACAMO and Very Low and Low Frequency Broadcast Builder (VBB) system. TACAMO-VBB is used at NCTS JAX to receive Emergency Actions Messages (EAMs) from the National Command Authority (the president and top military advisors) and transmit messages for rebroadcast to the triad of weapons delivery systems on constant alert.

"I'm proud that we play a key role in our country's command and control structure," said NCTS JAX Commanding Officer, CDR Eric McCartney. "In a day and age where fast, effective and concise communications

are the cornerstone of warfare on every front, NCTS JAX is more than ready to bear the responsibility of maintaining and operating such a critical system."

The addition of the TACAMO-VBB mission further bolsters NCTS JAX's goal to provide optimum customer service to support the needs of surface, sub-surface, air and ground forces deployed globally. America's TACAMO system became operationally deployed worldwide in 1969, offering a highly reliable and survivable means of communicating EAMs to all United States strategic forces.

Operating across every frequency band in the spectrum, utilizing multiple platforms to pass messages using a myriad of modulations, encryptions and networks, the TACAMO continues to provide the same service today. The system has seen many upgrades

since its first use and utilizes primarily aircraft to extend communications to surface, shore and sub-surface platforms across the globe, providing the capability to maintain contact with submarines, bombers and land-based missile sites.

"We have expert operators and technicians here to make sure our TACAMO and VBB systems remain operational 24/7/365 days a year," said LT Brian Harbin, NCTS JAX Electronics Maintenance department head. "The new install will ensure delivery of EAMs to strategic forces, maintaining our strategic deterrence and our national security."

For more information on the TACAMO system and its role in modern war fighting, visit www.tacamo.navy.mil. ✎

NIOC Misawa Sailors Celebrate Holidays with Local Orphanage

By CTR2 Melissa Kelley, NIOC Misawa

MISAWA, Japan -- In December, 40 Sailors and family members from Navy Information Operations Command (NIOC) Misawa attended the 47th annual Christmas party at the neighboring Akebono Orphanage. For more than 30 years, NIOC Misawa Sailors have sponsored the orphanage to the delight of both the children and the Sailors, and this year was no different.

The Sailors were greeted by the students and the festivities began with a welcome from the director of the orphanage, Mr. Toshimitsu Yokohama. The younger children performed a traditional Japanese dance, the older children did a pop song, and NIOC's own NC1 Arsenio Pabon teamed up with one of the students for a drum and bongo duet.

The entertainment was followed by a feast put on by both the orphanage and the Sailors, who brought some of their favorite holiday dishes to share with our Japanese hosts. Finally, Santa arrived, played by IT1 Kyle Carlson, and handed out gifts to each of the children who seemed to be just as excited by his visit as they were by the presents. They had provided their wish list and were sponsored by Sailors at the command.

Although NIOC Misawa has been



Official U.S. Navy Photo

directly involved with the orphanage for many years, the relationship between the orphanage and Misawa Air Base actually goes back to 1953. Every year, Sailors and families of NIOC Misawa participate in a number of events, including a Halloween party and pumpkin carving, Thanksgiving dinner, sports day, and the graduation of the older children in the spring.

Sailors at NIOC Misawa also hold fundraisers to provide a scholarship for the children who graduate from the orphanage at the end of their last year of high school. Sailors recently participated in a bike-a-thon

raising more than \$4,000 for the five students who will graduate in April.

The Christmas party is something that the entire command looks forward to every year according to NIOC Misawa Command Master Chief, CTRCM(SW) Matthew Bouchard. "The children were great and displayed exceptional hospitality to all," said Bouchard. "It was a joy to watch them play and interact with the Sailors and their families.

"The best part of the day was watching the joy on the children's faces as they got their gifts from Santa," said CTI2 Thomas Caniglia, a repeat volunteer. ✎

NGEN continued...

computer network for the Department of the Navy (DON). Created in 2000 to consolidate the disparate Navy networks into one collaborative Navy system, NMCI is one of the most transformational contracting initiatives ever undertaken by the DON.

Under Weller's direction, NMCI reduced seat cost and energy utilization while increasing capability and Information Assurance (IA) security. Today, the network maintains an availability of 99.8 percent for all users at any time, a significant improvement in NMCI's efficiency and effectiveness.

Weller was also personally involved in the negotiations for NMCI CoSC which began on Oct. 1, 2010. Under his leadership, the program office successfully executed a transition in which service was uninterrupted after the expiration of the NMCI contract. Also, the NMCI CoSC provides a structure that will enable the DON to transition to the future Next Generation Enterprise Network (NGEN) environment.

As Weller prepared for the transition, the advancement of NMCI continued as the program office accomplished a server virtualization

effort and implemented a large-scale Navy Enterprise Portal. The server virtualization reduced the number of physical servers by 2,200, lowering energy costs, reducing the network's IT footprint by 40 percent and cutting carbon emissions by 7,000 tons. The portal provides the Navy with the Department of Defense's most advanced, unified security model enabling information exchange that utilizes attribute-based access control and the capability to support one million users.

"Although the NMCI program is 10 years old, NMCI is a completely modern, five minute old network," Weller said. "We have upgraded and maintained NMCI with cutting-edge technology deployed on it since the beginning. All aspects of NMCI are state-of-the-art and state-of-the-shelf today. We are continuously advancing NMCI through the testing and deployment of new capabilities and security solutions."

EDITOR'S NOTE:

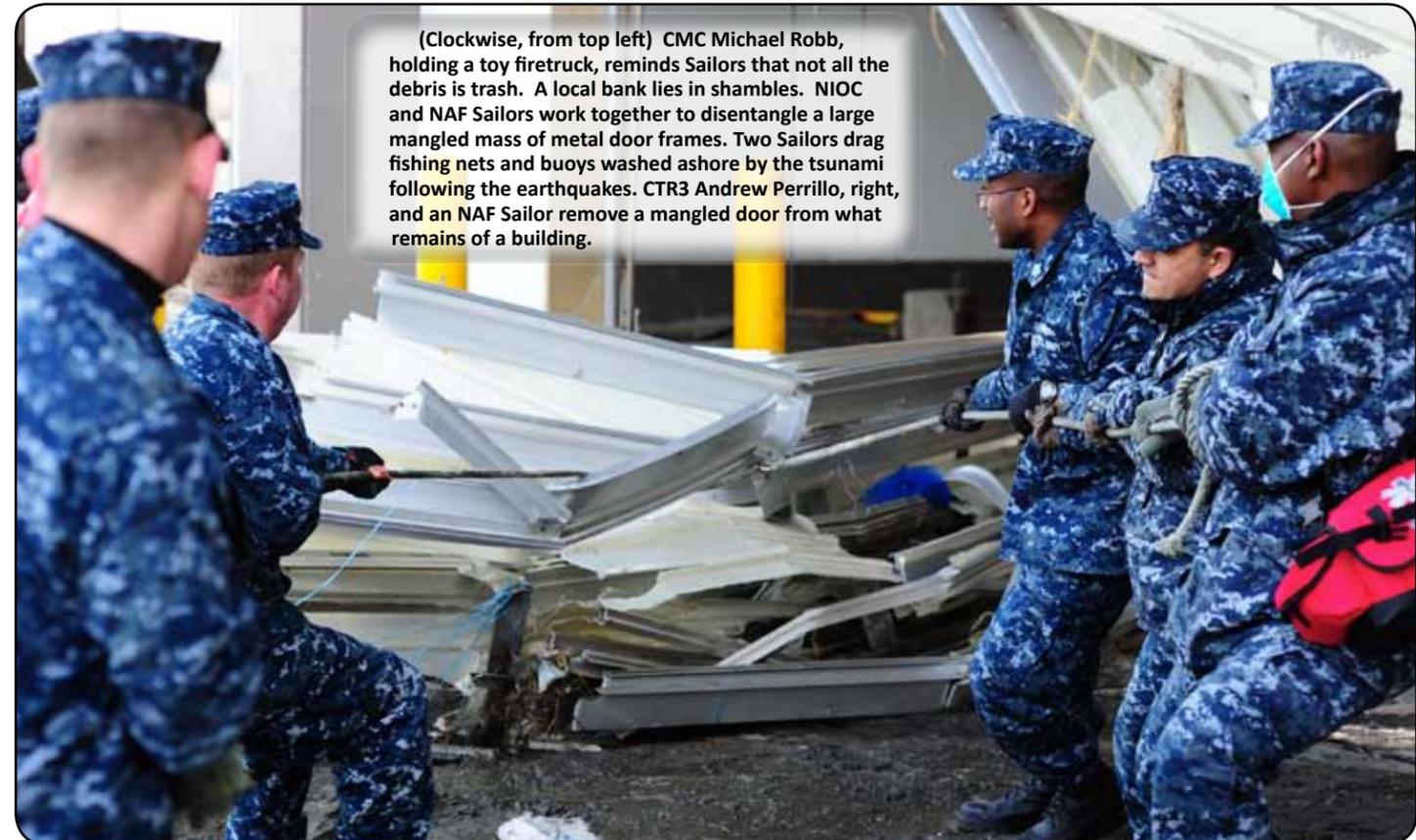
About the Navy Marine Corps Intranet

As a program of PEO-EIS, the Navy Marine Corps Intranet (NMCI) provides secure, seamless and global

end-to-end connectivity to more than 700,000 DON personnel at more than 3,000 sites in the continental United States, Hawaii and Japan. NMCI is a comprehensive information and communications network that replaced existing shore-based networks with one secure intranet, delivering access, interoperability and security through voice, video and data services.

About the Department of the Navy Chief Information Officer

The Department of the Navy Chief Information Officer (DON CIO) was established in 1997 to provide top-level advocacy in the development and use of Information Management (IM)/Information Technology (IT) and to create a unified IM/IT vision for the DON. The DON CIO develops strategies, policies, plans, architectures, standards and guidance and provides process transformation support for the DON. The DON CIO ensures that the development and acquisition of IT systems are interoperable and consistent with the Department's objectives and vision. For more information, please visit the DON CIO website: www.doncio.navy.mil.



(Clockwise, from top left) CMC Michael Robb, holding a toy firetruck, reminds Sailors that not all the debris is trash. A local bank lies in shambles. NIOC and NAF Sailors work together to disentangle a large mangled mass of metal door frames. Two Sailors drag fishing nets and buoys washed ashore by the tsunami following the earthquakes. CTR3 Andrew Perrillo, right, and an NAF Sailor remove a mangled door from what remains of a building.

NIOC Misawa Sailors Aid Japan

By CTI2(SW) Victoria L. Stack

MISAWA, JAPAN -- Following the devastating 9.0 magnitude earthquake and tsunami off the coast of Sendai, Japan, nearly 100 Sailors from Navy Information Operations Command (NIOC) Misawa and Naval Air Facility (NAF) Misawa joined to assist with cleanup operations and support for the devastated local community.

Despite continued aftershocks and disruptions to Misawa Air Base utilities operations, these Sailors were determined to do their part to help their Japanese hosts recover from the disaster.

"After everything that happened, I'm glad we finally have the opportunity to help," said CTR2 Irene Cencich from NIOC Misawa.

Sailors worked hand in hand, pulling trash and debris out of the administrative buildings and away from the beach. Many of the fishing nets washed ashore and were tangled with wood and garbage pulled up from the ocean.

"You don't really know how to react. It's all so surreal

— the amount of damage," said CTI2(NAC/SW) Kenneth Close. "There is so much mud and dirt ... and parts of boats washed all the way up in trees. It's hard to imagine how much damage Sendai and other cities must have."

Standing near one of the many beached fishing vessels, one fisherman said, "I am very lucky, out of all of my ships, none are damaged. Not everyone has been that lucky. Still, we are smiling, and we are glad for the help."

With all of the mud and debris left behind, restoration efforts will continue for some time. On day two of the cleanup, Chief Construction Mechanic Michael Robb reminded Sailors to stay safe while doing the best they could to restore the area.

"Remember, these are people's homes, these are their things," Robb said. "We're here to help them. Salvage as much as you can."

CTR3 Tiffany Young was grateful for the opportunity to serve. "It's amazing to watch and be part of helping them," she said. "It may take a while, but we're here, and that's important."



Photos by CTR2(NAC) Thomas Ahern



DEFENSE SUPERIOR SERVICE MEDAL

CAPT Philip Strozso, NSA/CSS Fort Meade



LEGION OF MERIT

CAPT Stephen N. Frick, NASA Johnson Space Center
CAPT Robert Goodwin, Jr., NCTS Far East
CAPT Alan Poindexter, NASA Johnson Space Center



DEFENSE MERITORIOUS SERVICE MEDAL

LT Kevin Barrett, NIOC Maryland
CTIC Anibal Bello, NIOC Texas
CDR Greg Braaten, NIOC Texas
CTR1 Vincent Campolo, COB Speicher, Iraq
CTRC Douglas Card, NIOC Maryland
CDR Christopher Chrislip, NIOC Sugar Grove
CTTC Clarence Covell, NIOC Menwith Hill
CTRC Brant Daggerhart, NIOD Yakima
CTNCM Christopher Dale, NIOC Maryland
CTNC Aimee Draughn, NIOC Texas
CTR1 Joshua DuFault, NIOC Maryland
CTICS Ryan Edwards, NIOC Hawaii
CTI1 Nory Gonzalez, NIOC Maryland
CTRC Janie Gray, NIOC Menwith Hill
YNC Jodi Hanlon, NIOC Hawaii
CWO3 Fredrick Kissling, NIOC Maryland
CTRC Marcus Kohlmann, NIOC Hawaii
CTRC Douglas Leoncavallo, NIOC Maryland
LCDR Robert Moore, NIOC Menwith Hill
CTRC Harrison Nash, NIOC Maryland
CTRC Michael Parks, NIOC Maryland
CTR1 Bradley Preston, CSG Joint Staff, Pentagon
CTR1 Misty Rambo, NIOC Maryland
ITC Kevin Stephens, NIOC Maryland
ITCS Latwaine Sweeper, NIOC Maryland
CTM1 Justin Thibou, NIOC Maryland
CTNC Peter Thomas, NIOC Texas
LTJG Mark Turner, U.S. Division South



MERITORIOUS SERVICE MEDAL

CAPT George Adams, CYBERFOR Virginia Beach
CDR Michael Bosley, NIOC Hawaii
LCDR Michael Brown, NIOC Norfolk
CDR Matthew Dean, NIOC Suitland
CWO5 David Dillon, NIOC Texas
CDR William Dodge, Jr., NIOC Whidbey Island
CDR Cheryl Gotzinger, NR NIOC HI Tacoma
CDR Steven Hudson, NIOC Norfolk
LCDR Michael Julch, NCTS San Diego

CAPT Glen Krueger, NR NIOC Maryland
CAPT Patrick Murphy, NETCENWARGRU Fort Meade
CDR Christopher Nerney, NR NETWARCOM Space
CDR Danny Noles, NIOC Bahrain
CDR William Rodgers III, NIOC Texas
CAPT Michael Roys, NR NETWARCOM Space
CDR Michael Seeberger, NR NCDOD
CDR Kevin Steck, NR NIOC North Island
CAPT Curtis Wold, NETCENWARGRU Fort Meade



AIR MEDAL

CTI1 Sean Roper, NIOC Bahrain



JOINT SERVICE COMMENDATION MEDAL

CTI2 Jennifer Aquino, NIOC Texas
Sgt Sean Barr, USMC, NIOC Hawaii
CTI3 Whitnie Bauer, NIOC Hawaii
MA1 Nicholas Berg, NIOC Hawaii
CTN1 Christopher Bisnett, NIOC Maryland
CTI2 Andrew Burdge, NIOC Maryland
LTJG David Cameron, COS Kalsu, Iraq
CTI2 Aneulena Candelaria, NIOC Hawaii
CTI2 Jedidiah Cates, NIOC Texas
CTR1 Ryan Causey, NIOC Maryland
CTR1 Chelsea Cooke, NIOC Hawaii
CTT1 Edward Cooper, NIOC Menwith Hill
CTI2 Jeremy Cummings, NIOC Hawaii
CTR2 Joseph D'Onofrio, NIOC Menwith Hill
CTR1 Christopher Epting, NIOC Maryland
CTI1 Richard Everson II, NIOC Maryland
LT Brandon Fason, NIOC Maryland
CTM2 John Furey, NIOC Maryland
CTI2 Matthew Galvin, NIOC Hawaii
CTI2 Kellynn Gorackowski, NIOC Maryland
CTN2 Kyle Griffith, NIOC Hawaii
CTR1 Zachary Gross, NIOC Maryland
CTI2 Daniel Hampson, NIOC Hawaii
CTRC David Harris, NIOC Maryland
CTI2 Shannon Hensley, NIOC Hawaii
CTR1 Alexander Hokanson, NIOC Maryland
CTI2 Galen Housley, NIOC Hawaii
SSgt Mary Jentz, USMC, NIOC Hawaii
CTR1 Kellie Johnson, NIOC Hawaii
LT Walter Johnson, NIOC Menwith Hill
CTN2 Micah Jones, NIOC Maryland
Sgt Timothy Lansing, USMC, NIOC Hawaii
CTR2 Tyler Lesser, NIOC Maryland
CTR1 Jason Lowes, NIOC Hawaii
CAPT Daniel MacDonnell, NIOC Maryland
CTR1 Dereck Marshall, NIOC Hawaii
Sgt Christopher Mason, USMC, NIOC Hawaii
CTN2 Jeffrey Music, NIOC Hawaii
MAC Dale Naaktgeboren, NIOC Sugar Grove
IT1 Nicolas Nannenga, NIOC Sugar Grove
CTR1 Alex Neil, NIOC Hawaii
IT1 John Peetz, NIOC Sugar Grove
CTR2 Rudolph Pekarovic, NIOC Maryland
CTR2 Bryan Plyter, NIOC Hawaii
CTR2 Wendell Proctor, NIOC Maryland
CTN2 Nancy Pugh, NIOC Hawaii

CTN2 Lance Pyle, NIOC Maryland
CTR1 Randal Rempfer, NIOC Maryland
YNC Jennifer Rivas, U.S. Joint Forces Command
CTN1 Jose Sanchez, NIOC Hawaii
CTN1 John Schulze, NIOC Hawaii
CTM2 Christopher Scott, NIOC Hawaii
CTI2 Luke Seaton, NIOC Hawaii
CTR1 Todd Sherwood, NIOC Menwith Hill
CTM1 Bryan Shoberg, NIOC Hawaii
CTM2 Patric Shoup, NIOC Hawaii
CTR2 Jeffrey Simon, NIOC Hawaii
CTN1 Terrance Smith, NIOC Maryland
CTI2 Sarah Sperling, NIOC Hawaii
CTN1 Derek Stevens, NIOC Hawaii
CTN2 Robert Tant, NIOC Maryland
CTR2 Bobby Thompson, NIOC Hawaii
CTMCM Kerby Thompson, COB Speicher, Iraq
CTN1 Patrick Voight, NIOC Texas
CTR2 Joshua Walter, NIOC Hawaii
CTI1 Joshua Weaver, NIOC Menwith Hill
CTR1 Curtis Wideman II, NIOC Menwith Hill
LT Kan Yang, NIOC Hawaii
CWO2 Daniel Yi, NIOC Hawaii
CTI1 Angel Zuleta, NIOC Menwith Hill



NAVY AND MARINE CORPS COMMENDATION MEDAL

YN1 Shuna Adams, NETWARCOM Virginia Beach
CDR David Archer, COMTENTHFLT Fort Meade
LT Jason Becker, NIOD Digby
ITCS Thomas Begley, NCTS FE Det Diego Garcia
CTI1 Charles Biles, NIOC Misawa
CTR1 Ricky Bourdeaux, Jr., NIOC Texas
ITC Andrew Bruhn, NCTS Naples
CTR1 Brandon Carter, NIOC Texas
LS1 Robert Cartwright, NCTAMS PAC Wahiawa
CTRCM Steven Chaney, NIOC Texas
CTTC William Cockrell, NIOC San Diego
CTNC Dave Collins, NCDOD
CTNC Kelvin Cook, NIOC Norfolk
LCDR Patricia Cregger, FLT/CYBERCOM Fort Meade
IT1 Jose Cruz, NIOC Texas
LCDR Wilfredo Cruzbaez, NETWARCOM Virginia Beach
CDR Suzanne Dalton, NETWARCOM Virginia Beach
OSC Jeffrey Davis, NR NETWARCOM Space
ETC James Dickson, NIOC San Diego
LT Jay Elson, NCTS Far East Yokosuka
LCDR Kevin Ernest, NIOC Maryland
CTT1 Marvin Ferguson, SPAWAR 0366
CTN1 Dustin Fritz, NIOC Suitland
CTICS Richard Fritz, NIOC Texas
CWO3 Stephen Garofolo, NIOC Texas
CTTC Bradley Glisan, NIOD Jacksonville
CTNCS Matthew Golden, NIOC Pensacola
ET1 David Gose, NCTAMS PAC Wahiawa
CTTCM Jeffrey Harris, NR COMTENTHFLT Fort Meade
CTIC Stephanie Harris, NIOC Texas
LT James Herzog, NCTAMS LANT Norfolk
CTTC Jesse Hess, NIOC Hawaii
LCDR Corey Hesselberg, NETWARCOM Virginia Beach
ET1 Fred Holmes III, NIOC Norfolk
CTMCS Naomi Hough, CID ARI Corry Station
ITCS Richard Huerta, Jr., NIOC Texas
LCDR Michael Jones, NR NETWARCOM Space
YNC Tracy Kelso, CYBERFOR Virginia Beach

LT Kirstein Lewis, NCTS Sicily
LCDR Miguel Macias, NCTAMS PAC Wahiawa
LT James Marsh, NCTS Sicily
CTNC Mark Megna, NIOC Norfolk
CTI1 Jesse Meunier, NIOC Texas
YNC Corey Mincey, NCTAMS PAC Wahiawa
CTIC Paul Minuti, NIOD Digby
CTI1 Omaira Morales, NIOC Texas
LT Stephanie Muskovac, NIOC Norfolk
CTRC Brian Niebauer, NIOC Hawaii
CTTC Shon O'Connell, NIOC Georgia
CTIC Julie Pierrelousegzi, NIOC Texas
CMDM Terry Piper, NIOC Hawaii
CTMC Ricky Pottebaum, NIOD Groton
CTI1 Jessica Powers, NIOC Texas
CTMCS Michael Prieto, NR NIOC GA Greensboro
CTNCM Kevin Radzewicz, NIOC Norfolk
ITCS Sonya Rivera, NCTAMS LANT DET Hampton Roads
IT1 Gary Rose, Jr., NCTS FE Det Misawa
ET1 John Ruttly, CYBERFOR Virginia Beach
ET1 Jonathan Salzer, NCTSC Det Fairfield
ITC Luisa Santana, NCTS FE Det Chinhae
CDR Christopher Saufley, CYBERFOR Virginia Beach
CSC Christopher Shearin, NIOC Georgia
ITC Joe Simmons, CYBERFOR Virginia Beach
CTNCS Jeffrey Smith, NIOC Pensacola
CTN1 Terrance Smith, COMTENTHFLT Fort Meade
LT Theodore Smith, NR NIOC TX
CTN1 Robert Stappert, Jr., NCDOD
CTNC Tammy Sternberg, NCDOD
CDR Brian Talicuran, NR NCTAMS LANT Norfolk
CTICM Steven Tallman, NIOC Texas
LT Brian Tichenor, NIOC Texas
CTTC Alicia Tuft, NIOC San Diego
CDR Michael Van Poots, Navy Reserve Naval Security Force Sugar Grove
CTNC David Vano, NETCENWARGRU Fort Meade
CTNCS Edward Walker, NIOC Georgia
YNCS Kermit Westfall, NCTAMS LANT DET Hampton Roads
ITC Dewayne Williams, NCTS FE Yokosuka
MAJ Deangelo Willis, USMC, NIOC Norfolk
CDR Marcia Ziemba, NCTAMS PAC Wahiawa



JOINT SERVICE ACHIEVEMENT MEDAL

IT3 Kristina Acosta, NIOC Hawaii
IT2 Cory Allen, NIOC Hawaii
IT1 Harold Andrews III, NIOC Georgia
CTN2 Chad Arnold, NIOC Maryland
CTI2 Kristen Baker, NIOC Hawaii
CTR2 Patrick Barnick, NIOC Hawaii
SGT Mark Barratt, USMC, NIOC Hawaii
CTI1 Heather Barron, NIOC Georgia
CTR1 Jason Bates, NIOC Sugar Grove
SGT Guy Bernal, USMC, NIOC Hawaii
MA3 Travis Braun, NIOC Hawaii
CTN2 Taia Burngasser, NIOC Hawaii
CTR2 Cody Camou, NIOC Sugar Grove
LT Joey Carter, NIOC Texas
CTNC Robert Couey, NIOC Maryland
CTI1 Dominique Covarrubias, NIOC Texas
CTR2 Keith Curley, NIOC Hawaii
CTR2 Samuel DiFrancis, NIOC Maryland

CTM2 Andrew Duhe, NIOC Maryland
IT2 Jedidiah Dyer, NIOC Hawaii
IT2 Tovress Eley, NIOC Maryland
CTR2 Erik Faulk, NIOC Hawaii
CTR2 Seth Ferguson, NIOC Texas
CTR3 Darren Fitzgerald, NIOC Sugar Grove
ITSN Ashley Flannery, NIOC Hawaii
CTM3 Scott Fortin, NIOC Maryland
CTM2 Michael Gustafson, NIOC Hawaii
CTR2 Michael Hayslett, NIOC Hawaii
LCDR Dorothy Hinkley, NIOC Hawaii
CTI1 Chad Hora, NIOC Georgia
CTI2 Jessica Hornsby, NIOC Georgia
CTR2 Ryan Jones, NIOC Sugar Grove
CTR2 Brittney Kramberg, NIOC Hawaii
CTR2 Joseph Kramer, NIOC Maryland
CTT1 Nicholas Lawson, NIOC Menwith Hill
CTIC Olga Levkovich, NIOC Maryland
CTR2 Kimberly Martin, NIOC Hawaii
CTR2 Ralph Matheny, NIOC Hawaii
CTR1 Nicholas McConnell, NIOC Hawaii
CTN2 Gregory Park, NIOC Maryland
CTN1 Dale Pfaff, NIOC Maryland
CTI3 Nicholas Polen, NIOC Maryland
YN1 Keith Rainey, CSG Baghdad
IT1 Franklin Shaw, NIOC Sugar Grove
IT2 Heather Shear, NIOC Hawaii
CTI2 Kevin Shirkey, NIOC Hawaii
IT2 Jacy Smith, NIOC Maryland
CTN1 Kevin Sroka, NIOC Hawaii
CTI2 Ashley Stone, NIOC Hawaii
CTT1 Carly Story, COMNAVFORKOREA
CTN2 Albert Su, NIOC Hawaii
CTR1 Adam Swain, NIOC Georgia
CTM2 Zachary Thomas, NIOC Hawaii
CTM3 Tanesha Thompson, NIOC Hawaii
CTI1 Jessica Trujillo, NIOC Georgia
CTI2 Javaise Vezia, NIOC Hawaii
CTM2 Bradley Wakefield, NIOC Hawaii
CTR2 Ryan Walker, NIOC Sugar Grove
CTT2 Robert Williamson, NIOC Hawaii
CTR3 Jeffrey Worcester, NIOC Sugar Grove



NAVY AND MARINE CORPS ACHIEVEMENT MEDAL

ET2 Charles Anderson, Jr., NCTAMS PAC Wahiawa
ITC Robert Armenta, Sr., NCTS San Diego
CTN1 Michael Bedwell II, NCDOD
IT2 Tasha Beverly, NCTS Far East Yokosuka
CTR1 Ryan Birn, NR NIOC Greensboro
CTM2 Peter Bosserman, NIOC Norfolk
CTR2 Jacob Branch, NIOC Hawaii
IT3 Brittany Brandon, NIOD Groton
IT1 Matthew Brashares, NCTS FE Det Diego Garcia
CTI1 Ryan Bristol, NIOC Misawa
CTI1 Kelley Brown, NIOC Georgia
CTM2 Matthew Brown, NIOC Norfolk
IT1 Rachel Brown, NMCI DET San Diego
CTI2 Matthew Bruner, NIOC Maryland
IT1 Todd Brunner, NCTAMS LANT DET Souda Bay
CTI1 Ronald Burk, Jr., NIOC Georgia
CTI1 Kelly Butler, NIOC Georgia
CTI2 Alicia Campbell, NIOC Texas
CTTC Miltayon Campbell, NIOC Norfolk
CTI1 Amanda Carter, NIOC Bahrain

CTI1 Justin Carter, NIOC Bahrain
CTI1 Scott Carter, NIOC Georgia
CTM2 Zachary Carver, NIOC San Diego
LCDR Miguel Castellanos, COMTENTHFLT Fort Meade
CTM2 Zacquekine Chandler, NIOC Yokosuka
CTT1 Richard Chellette III, NIOC Norfolk
CTN1 Byron Clayton, Jr., NIOC San Diego
LSC Yvonne Cole, NCTS Sicily
CTI2 James Collins, NIOC Texas
CTI2 Nathaniel Connolly, NIOC Bahrain
IT1 Arrieanne Copeland, NMCI DET San Diego
CTR1 Edwin Cordero, NIOC Hawaii
CTN1 Christopher Crabtree, NCDOD
LT Hollie-Noelle Cronley, NIOC Hawaii
CTR2 Zandria Curran, NIOC Hawaii
IT2 Michael Dobschuetz, NCTAMS LANT Norfolk
CTR1 Robert Dudas, NIOC Suitland
CTR1 Nicole Duran, NIOC Yokosuka
IT2 Candie Durham, NCTS FE Yokosuka
CTM2 John East, NIOC Norfolk
ET1 Angelo Echevarria, NCTS Jacksonville
IT2 Jonathan Ellison, NIOC Yokosuka
IT2 Kawana Elrod, NCTAMS PAC Wahiawa
IT2 Harlan, Famisan, NCTS FE Det Okinawa
LS2 Nicole Ferreira, NCTAMS LANT DET Rota
CTI2 Benjamin Fewkes, NIOC Bahrain
CTI1 Laura Folk, NIOC Maryland
CTI2 Shannon Forbes, NIOC Hawaii
CTI1 Timothy Franklin, NIOC Hawaii
CTM1 Charles Frederick, NIOC Hawaii
IT1 Nicholas Friedrich, NMCI DET San Diego
YN2 Angelina Gabriel, NIOC Maryland
ET2 Eric Gaebel, NCTS San Diego
YN2 Elise Garnier, NIOC Hawaii
CTN2 Brendan Gillespie, NCDOD
LT Robert Gonzalez, NCTAMS PAC Wahiawa
IT1 Loushawda Grant, NCTS Jacksonville
CTT2 Nathaniel Grau, NIOC Georgia
YN2 Skyler Graves, NCTS FE Det Misawa
IT3 Marc Gurule, NCTAMS PAC Wahiawa
CTI1 Natalie Hammond, NIOC Bahrain
CTR1 John Hammonds, NIOC Hawaii
IT2 Jonah Harper, NCTAMS LANT Norfolk
YN2 Demetric Hart, NIOC Hawaii
CTR1 Cory Hays, NIOC Georgia
CTM1 Stephen Huber, NIOC Hawaii
IT3 Daniel Johns, NCTSC Det Patuxent River
CTI2 Kyle Kane, NIOC Maryland
CE1 Gary Kesterson, NCTS FE Det Sasebo
YN3 Mark Konrad, NIOC Norfolk
IT1 Rhiannon Kronberg, NCTAMS LANT Norfolk
CTT1 Ketri Landrum, NIOC San Diego
LTJG Nicholas Lange, NIOC Georgia
ET1 Michael Larson, NCTS FE Det Okinawa
IT1 Billy Lewis, NCTAMS PAC Wahiawa
LTJG Marcus Long, NIOC Hawaii
ET1 Joseph Machado, NCTS FE Det Okinawa
ET1 Monseise Madrigal, NCTS FE Det Diego Garcia
CTR3 Phillip Mahoney, NIOC Suitland
CTT2 Christopher Martin, NIOC Georgia
IT2 Christopher Martinez, NCTSC Det Oklahoma City
YN2 Daniel Martinez, Jr., NMCI DET San Diego
CTN2 Shawna Maynard, NIOC Hawaii
IT2 Brandon McMurtrie, NCTSC Det Fairfield
CTM1 Matthew Messner, NIOC Hawaii
CTI1 Jennifer Miller, NIOC Maryland
CTM2 Brian Mills, NIOC San Diego
IT3 Britney Moore, NCTAMS PAC Wahiawa
IT2 Tony Nelson, NCTAMS LANT Norfolk
CTN1 Andrew Nguyen, NIOC Hawaii
LTJG Melissa Ocasio, NIOC Hawaii

CE2 Rodney Pelangka, Jr., NCTS FE Det Atsugi
 CTT2 Michael Perry, Jr., NIOC Hawaii
 CT11 Jinwei Pho, NIOC Hawaii
 OS2 Veronica Powell, NCTAMS LANT Norfolk
 CTN2 Gregory Price, NIOC Hawaii
 ET1 Ravin Rambaran, NCTS Naples
 CE1 Bienvenido Ramos, NCTS FE Det Diego Garcia
 LS3 Paul Rivera, NIOC Maryland
 IT1 Marisette Rodrigez, NCTS Jacksonville
 CT12 Preston Rodriguez, NIOC Georgia
 CTN1 Ryan Rolfe, NIOC Hawaii
 YN2 Jodi Salazar, NCTAMS PAC Wahiawa
 IT1 Salvador Sanchez, NCTS San Diego
 YN1 Nena Sanders, NIOC Misawa
 IT1 J Schmidt, NCTAMS LANT DET Hampton Roads
 CTR2 Jamie Schulze, NIOC Hawaii
 CTR1 Jason Scofield, NIOC Georgia
 CTNSN Matthew Seefeldt, NIOC Hawaii
 IT1 Marlene Serrano, NCTAMS LANT Norfolk
 LT Kevin Shackelford, NIOC San Diego
 ITC Sandra Shannon, NCTS San Diego
 CTR1 Michael Shost, NIOC Texas
 CT11 Jason Sikora, NIOC Bahrain
 IT2 April Simon, NCTS San Diego
 CT12 Charissa Skuza, NIOC Georgia
 CT11 David Smart, NIOC Texas
 CTN1 Charley Snyder, NIOC Texas
 CT11 John Sobery, NIOC Texas
 CT11 Virginia Soto, NIOC Texas
 ET1 Gary Spigarelli, NCTSC Det Oklahoma City
 CM2 Kensey Stephens, NIOC Hawaii
 ET2 Nicolas Stersic, NCTS FE Det Diego Garcia
 CTR1 Matthew Strauss, NIOC Bahrain
 CTR2 Lauren Suddreth, NIOC Hawaii
 CTR1 Mathew Takae, NIOC Yokosuka
 CT12 Jesse Tant, NIOC Georgia
 CTM2 Stephen Tierney, NIOC Norfolk
 CTR1 Terry Tillie II, NIOC Bahrain
 CT12 James Toole, NIOC Texas
 CT11 Clieveral Troxler, NIOC Bahrain
 ET1 Richard Truchanowicz, NCTS FE Yokosuka
 CTTCS Peer Tuckson, NCDOD
 IT2 Jennifer Turnbull, NIOC Bahrain
 CT12 Jeremy Turner, NIOC Texas
 CTR1 Jennifer Valentin, NIOC Bahrain
 CTN1 Nathan Vidal, NIOC Maryland
 CT11 Anthony Walter, NIOC Bahrain
 CTR1 Bryan Walters, NIOC Texas
 IT1 Damien Washington, NIOC Bahrain
 CTN1 Sha-nicca White, NCDOD
 ET1 William White, NCTAMS PAC Wahiawa
 CT12 Christine Williams, NIOC Texas
 CTT2 Gary Wong, NIOC San Diego
 CTT1 Daniel Yanklowitz, NIOC San Diego



**MILITARY OUTSTANDING
 VOLUNTEER SERVICE MEDAL**

NC1 Theresa Aguayo, NCTAMS PAC Wahiawa
 CTR1 Miriam Samuels, NIOC Georgia

**CIVILIAN LENGTH OF
 SERVICE AWARDS**

Etta Coleman, NETWARCOM VA Beach - 36 Years

Sylvia Cuffee, GNOC DET Norfolk - 30 Years
 J Kenyetta Rodgers, NETWARCOM VA Beach - 25 Years
 Charles Kiriakou, NETWARCOM VA Beach - 20 Years
 Dennis Wakmunski, NETWARCOM VA Beach - 20 Years
 Kenneth Washington, NETWARCOM VA Beach - 15 Years
 Jackie Davis, GNOC DET Norfolk - 10 Years
 Louis Weiss, NETWARCOM VA Beach - 10 Years



NETWARCOM Commander Named Federal 100 Recipient

By John Donaldson, NETWARCOM Public Affairs Officer

VIRGINIA BEACH, VA – Federal Computer Week has announced RADM Edward H. Deets III, Commander, Naval Network Warfare Command (NETWARCOM), as one of the recipients of the 22nd annual Federal 100 Awards. These awards are presented to the top 100 government, industry and academic leaders who have played pivotal roles in how the federal government acquires, develops and manages Information Technology (IT).

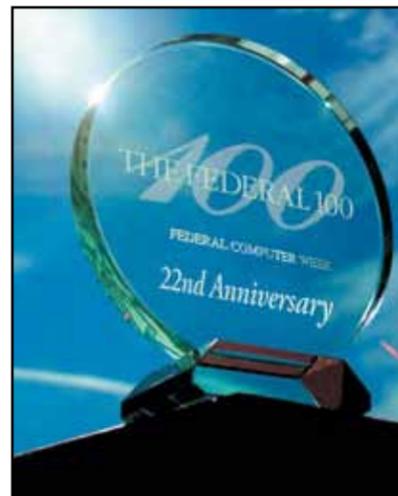
Deets was recognized for his leadership of the Navy's Information Warfare and Cryptology Community of more than 11,000 personnel and also as the NETWARCOM Commander, leading the operation of the Navy's networks that provide vital services to 750,000 users. His



RADM Edward H. Deets III

visionary leadership, experience and technical ability were critical to delivering network services, long haul communications and space capabilities to naval and joint warfighters across the globe.

Deets also directed efforts to identify more than 1,300 'legacy' networks that lacked full and effective defensive capabilities to combat hostile intrusions. His work resulted in the termination of more than 970 of these vulnerable networks, vastly improving security posture and generating a savings of more than \$20 million to date. He consistently fosters an environment of teamwork and quality service inspiring everyone to achieve at the highest level. ✎



COMTENTHFLT Announces 2010 On-The-Roof Gang Annual Award

From FLTCYBERCOM/C10F Public Affairs

FORT MEADE, MD -- VADM Bernard J. "Barry" McCullough, commander, U.S. Fleet Cyber Command and U.S. 10th Fleet recently announced the winners of the 2010 On-The-Roof Gang (OTRG) award which was established for cryptologic excellence by the OTRG association.

Between the years 1921 and 1927, several U. S. Navy and Marine Corps personnel taught themselves to break Japanese code and passed these skills informally to many of their contemporaries.

The value of the information extracted was recognized, and under the auspices of Op-20-G, the former Office of the Director of Naval Communications, formal training was developed and implemented in 1928. Until 1941, this activity took place in a specially constructed block house on the roof of the old main Navy building in Washington, DC, hence the name 'On-The-Roof' Gang.

The Navy OTRG winner is CTTM(SW/AW/EXW/FPJ) Larry H. Dean, COMNAVSPECWARDEVGURU.

The Marine Corps OTRG winner is MSgt. James B. Hillyer, USMC, Company A, 1st Radio Battalion.

"To be nominated for the OTRG award was an absolute honor in itself," said Dean. "My selection is not solely a

reflection of my contributions, but more of a reflection of the sound leadership and guidance that I have been fortunate to have in my past 24 years as a cryptologist."

"These outstanding information warriors and cryptologists exemplify leadership, initiative, resourcefulness and dedication, and personify the highest traditions," added McCullough.

EDITOR'S NOTE: *As always, the competition was very tight for these honors. Congratulations also go to the following nominees for their significant contributions to the Navy and the nation: CTRC(SW) Adam D. Bass, USS Gettysburg (CG 64); CTNCS(IDW/PJ) Jeremiah J. Hanks, NIOC Maryland; CTTCS(SG) Brady G. Labrum, NIOC Hawaii; CTRC(SW/AW) Shawn A. Modisette, NIOC Menwith Hill; CTNCS(IDW/FPJ) Neil S. Rubin, NIOC Maryland; CTTCS(SW) Thadeus Szynski, USS Chafee (DDG 90); CTTCS(IDW/SW/AW) Kimberlee D. Thompson, NIOC Colorado; CTNCS(IDW) Ethan W. Waters, NOIC Texas; CTIC(AW/SW/NAC) Michael C. Wang, NIOC Misawa, Japan; CTN1(SW) Robert B. Wolf, NIOC Pensacola; and MSgt. Leif T. Landa, USMC, 1st Radio Bn., 1 Marine Headquarters Group, 1 Marine Expeditionary Force. ✎*

WWII Code & Cipher School Serves as Backdrop for Pinning Ceremony

From NIOC Menwith Hill Public Affairs

During World War II, Bletchley Park, England was home to the Government Code and Cipher school. Here, such notables as Alan Turing developed ground breaking equipment like the Bombe and Colossus to decrypt German Enigma and Lorenz ciphers.

The school provided vital intelligence to the strategic decision makers and military commanders. Similarly as effective to the Allied effort and during the same time period, May 1943 to June 1945, U.S. Tenth Fleet stood up with an Anti-Submarine Warfare mission targeting German U-Boats.

It was Tenth Fleet that had an immediate and sustained impact throughout the remainder of World

War II in the number of U-Boats that were destroyed.

In 2010, the Information Dominance Corps saw the reactivation of U.S. Tenth Fleet and the information domain as a recognized warfare area with warfare qualification and insignia.

Thus it was fitting for the officers of Command Task Group (CTG) 1000.1 Navy Information Operations Command (NIOC) Menwith Hill and CTG 1060.2 Fleet Information Operations Center (FIOC) United Kingdom, under the commander, U.S. Tenth Fleet and Cryptologic Support Group Molesworth to revisit the past and conduct their Information Dominance Warfare

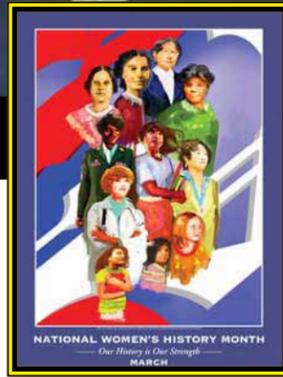
Officer pinning ceremony at Bletchley Park.

Following a tour of the grounds, CDR Timothy May, commanding officer, NIOC Menwith Hill was pinned and then pinned his 10 fellow officers.

Even within the new opportunities and challenges within the Cyber arena that are at the forefront, the same fundamentals from World War II still apply.

Individuals who possess a strong technical foundation, understand the operational environment for it to be applied, and can relay this to their warfighting commanders, will always have significant relevance to the military and national security efforts. ✎





Women Contribute to Naval Service for more than 100 Years

From the Office of the Chief of Naval Operations

March is Women's History Month. The theme for national and Department of Defense (DoD) observances this year is "Our History is Our Strength."

Women's History Month originated in 1978, when the Sonoma County (California) commission on the status of women initiated a Women's History Week to coincide with international Women's Day. In 1981, in response to growing support for the observance, Congress passed a joint resolution proclaiming a Women's History Week.

In 1987, the National Women's History Project, a nonprofit organization dedicated to honoring and preserving women's history, petitioned Congress to expand the celebration to the entire month of March. Since then, National Women's History Month has been celebrated annually, in commemoration of the diverse contributions women have made, and continue to make, to our nation.

Today, more than 53,000 active-duty women and more than 10,000 female reservists are serving in the Navy. At 16.3 percent of the force, they make indispensable contributions to our mission and operations. Thirty-one active and Reserve female flag officers and more than 50 female command master chiefs are leading from the front.

Nearly 50,000 women serve in a wide range of specialties as Navy civilians. Today, 95 percent of Navy billets are open to women; and women are assigned to ships, afloat staffs, naval construction force units and aviation squadrons.

Since becoming an official part of the Navy in 1908 with the establishment of the Nurse Corps, women have exerted an ever-

increasing influence and impact. With the passage of the Women's Armed Services Integration Act (WASIA) on 12 June 1948, women gained permanent status in the armed services.

The first six enlisted women were sworn into the regular Navy in July 1948 and, in October of that year, the first eight female officers were commissioned. Women were first assigned to selected non-combatant ships in 1978, and opportunities were later broadened in 1994 to include service on combatant ships following the repeal of the combat exclusion law. Most recently, in April 2010, the Navy announced a policy change that allows women to serve on submarines.

The spirited and courageous efforts of women in the United States Navy have shaped our naval history. A veteran of two World Wars and director of the Women Accepted for Volunteer Emergency Service (WAVES) from 1946 to 1953, CAPT Joy Bright Hancock played a critical role in the passage of WASIA.

During the Vietnam War in 1972, CDR Elizabeth Barrett became the first female Line officer to hold command in a combat zone when she became commanding officer of the Naval Advisory Group in Saigon. In 1974, LT Barbara Allen Rainey earned her wings, becoming the first female U.S. naval aviator. In 1990, LCDR Darlene Iskra became the first woman to command a Navy ship and, in 1998, CDR Maureen A. Farren became the Navy's first female combatant ship commander.

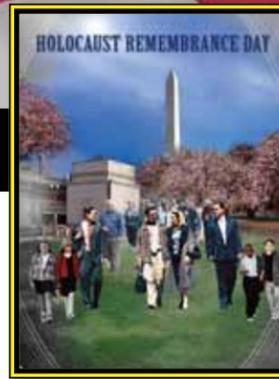
In 2002, Master Chief Jacqueline Dirosa became the Navy's first female Force Master Chief and, in 2006, she became the first female Fleet Master Chief. CAPT Sunita Williams, a naval aviator and NASA

astronaut, set the record in 2007 for the longest uninterrupted space flight by a female astronaut. All commands are strongly encouraged to increase their knowledge and awareness of the contributions of women to our Navy and nation by celebrating Women's History Month through programs, exhibits, publications and participation in military and community events.

A presentation is available on the Defense Equal Opportunity Management Institute website at <http://www.deomi.org/specialobservance/presentations.cfm?catid=3>. Materials on the role of women in naval history can be found at <http://www.history.navy.mil/special%20highlights/women/women-index.htm> and <http://cmsauthor.bupers.navy.mil/aboutus/bupers/womenspolicy/womenshistorymonth.htm>.

Information on the contributions of women to our nation's legacy can be found at <http://womenshistorymonth.gov/> and <http://nwHP.org/>.

More information on diversity conferences, events and observances is available at the Navy Diversity website: <http://www.npc.navy.mil/commandsupport/diversity>.



National Days of Remembrance

FREQUENTLY ASKED QUESTIONS:

What is Days of Remembrance?

The U.S. Congress established Days of Remembrance as the nation's annual commemoration of the Holocaust and created the United States Holocaust Memorial Museum as a permanent living memorial to the victims.

This year, Holocaust Remembrance week is May 1 through May 8, 2011. The Museum designated "Justice and Accountability in the Face of Genocide: What Have We Learned?" as the theme for the 2011 observance. In accordance with its congressional mandate, the Museum is responsible for leading the nation in commemorating Days of Remembrance and for encouraging appropriate observances throughout the United States.

What is the Holocaust? Who are we remembering?

The Holocaust was the state-sponsored, systematic persecution and annihilation of European Jewry by Nazi Germany and its collaborators between 1933 and 1945. Jews were the primary victims—six million were murdered; Roma (Gypsies), people with disabilities, and Poles were also targeted for destruction or decimation for racial, ethnic or national reasons. Millions more, including homosexuals, Jehovah's Witnesses, Soviet prisoners of war, and political dissidents, also suffered grievous oppression and death under Nazi Germany.

What is the significance of this year's Days of Remembrance theme?

This year's Days of Remembrance theme, "Justice and Accountability in the Face of Genocide: What Have We Learned?" commemorates the 65th anniversary of the verdicts delivered at the International Military Tribunal in Nuremberg and the 50th anniversary of the Eichmann trial.

The theme marks these anniversaries and encourages reflection on the role of justice in the aftermath of genocide. Both trials set important precedents and raised significant questions about the nature of justice in the face of such enormous crimes. Prior to the International Military Tribunal and subsequent Nuremberg trials, the principle of national sovereignty prevailed; in its aftermath, a new understanding of international responsibility for human rights would emerge as the world began to fully understand the events now called the Holocaust.

Adolf Eichmann was a high-ranking SS (Schutzstaffel, or elite guard of the Nazi party) officer central to the

planning and implementation of the murder of six million Jewish men, women and children. He was captured in Argentina by Israeli agents in 1960 and brought to trial in Israel for what would become known as the "trial of the century."

It was a watershed event televised around the world, refocusing international attention on the murder of Europe's Jews. The Nuremberg and Eichmann trials strove for justice, but what does justice really mean in the face of a crime like genocide? The trials were an act of public accountability owed to the victims; justice to a great extent was aspirational.

How can I participate in Days of Remembrance?

Every year during Days of Remembrance, ceremonies and activities are held throughout the United States—in local communities; at state and local government offices; on military bases; and in workplaces, schools, churches and synagogues.

You may be able to take part in a commemoration already planned in your community, or if such a community-wide event is not currently planned, you may encourage your local and state officials to issue a proclamation indicating their support for commemorating these events.

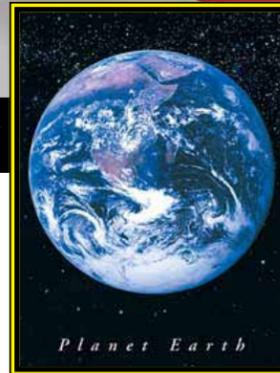
For sample state and city proclamations, visit www.ushmm.org/remembrance/dor/organize. For information about the many other ways to get involved, please review the materials in the Planning Guide, or visit the Museum's Website, www.ushmm.org/remembrance/dor.

Can we participate in Days of Remembrance events at the Museum or the U.S. Capitol?

The United States Holocaust Memorial Museum welcomes attendance at its Names Reading ceremony, which takes place in the Museum's Hall of Remembrance throughout Holocaust Remembrance week. The National Days of Remembrance Ceremony held at the U.S. Capitol Rotunda can be viewed live on the Museum's Website, www.ushmm.org.

Where can I find more resources for a Days of Remembrance commemoration or general information on the Holocaust?

Please visit www.ushmm.org.



New Diversity Officer Stays the Course

As Navy Cyber Forces Diversity Officer, I look forward to building on the Navy's five established Pillars of Diversity – Accountability, Outreach, Mentorship, Communication and Training – to enhance our domain Diversity program. As you review our initiatives that follow, please consider how you can get involved to help us maintain a working environment throughout the domain that values and leverages the unique capabilities and perspectives that each of us bring to the team.

Under the **Accountability** Principle, we are establishing a new awards program to recognize all nominated domain personnel for their outstanding diversity efforts. All nomination packages for the various diversity awards will be reviewed at CYBERFOR. The individual with the strongest nomination package for each award will receive a Flag Letter of Commendation (FLOC) and



LCDR Christine A. Cochran

their package will be forwarded with the Type Commander's (TYCOM's) endorsement: this includes those packages that do not require a formal endorsement letter. All other nominees will receive a Letter of Appreciation (LOA) from the Chief of Staff. In addition to receiving LOC's and LOA's, all enlisted members will receive recognition from the Force Master Chief. For those awards that do not require an endorsement

letter, we will forward all packages received, in addition to the package endorsed, to the organization that is sponsoring the award so all members have the opportunity to compete for the award.

For **Outreach**, I will lead the expansion of our efforts to include the Hampton Roads NROTC Units located at Old Dominion University, Hampton University and Norfolk State University. My primary focus will be to build relationships between the Midshipmen/Officer Candidates and members of the Information Dominance Corps (IDC). Specifically, we will participate in the leadership forums, career days and NROTC classes held for the Officer Candidates and Midshipmen.

While we will maintain our current Partnership agreement with Churchland Middle School to provide tutoring and mentoring to the younger students, it is also important that we reach out at the University level to provide information about the IDC and what we do.

Also as part of our **Outreach** efforts, RADM Meek and other members of our executive

leadership team will attend Diversity events across the country to raise awareness of the importance of Information Dominance work in the Navy, as well as how diversity programs enhance our ability to accomplish CYBERFOR's mission.

Our **Mentorship** instruction was signed 7 Jan., so our mentor program will be in full swing this year. The instruction gives all commands one year to have their mentors trained and their program up and running. Some Mentor Program Coordinators (MPCs) have already started the training, and others will have the opportunity to receive their certification training at the Association of Naval Services Officers (ANSO) Symposium in May. Additionally, we have also developed

a program to prepare protégés to establish a healthy and enduring relationship with their mentors. We expect this to be a very successful program.

Diversity **Communication** is an area in which we have excelled. We were one of the first TYCOMs to set regularly scheduled Diversity Council meetings, chaired by the Chief of Staff on a monthly and quarterly basis. The monthly meetings are held at the headquarters level with participants from both CYBERFOR and Naval Network Warfare Command (NETWARCOM), and the quarterly meetings include domain Diversity personnel. We will continue to hold these meetings regularly to ensure that everyone is getting the latest word on what is going on in the world of Diversity.

Lastly, under the **Training** Principle, we had Monica Emerson, Navy Diversity Officer; conduct our Executive Leadership Training on 30 March for CYBERFOR and our subordinate commands in the local area. The training proved to be a

big success and provided us with a great opportunity. We are waiting for an update to the Navy's Diversity comper based training. Once that is completed, we will disseminate that information throughout the domain. The Appreciating Differences class is held regularly at Joint Expeditionary Base Little Creek, and is mandatory for all headquarters E7 and above and supervisors. We have five remaining classes scheduled for this year, and information is available by contacting the CYBERFOR Training Officer. To date, 136 Sailors and civilians from CYBERFOR and NETWARCOM have completed the class, offering very positive reviews.

As many of you are aware, LCDR Mark Venzor worked tirelessly to establish the strong domain Diversity program that we now enjoy – however, much work remains. I ask for your assistance in taking this initiative to the next level. Together, we will ensure that CYBERFOR remains the model for Diversity in the Navy. ✌

UPCOMING DIVERSITY CONFERENCES

CONFERENCE	LOCATION	DATES	WEBSITE
HR & EEO in the Federal Workplace Conference	Washington, DC	Apr 4-6	www.fedhrconferences.com
Midwest Asian American Student Union (MAASU)	Twin Cities, MN	Apr 8-9	
Diversity Professional Certification (CDP) Training	San Francisco	Apr 19-22	www.dtui.com/conferences.html
Federal Asian/Pacific American Council (FAPAC) National Leadership Training Conference (Hyatt Regency)	Bellevue, WA	May 9-13	
Diversity in Challenging Times	TBD	May 25	www.diversityconferences.org.uk/index.html
7th Annual NAACP Leadership 500 Summit (Westin Diplomat Hotel)	Hollywood, FL	May 27-30	
National Conference on Race and Ethnicity in American Higher Education (NCORE)	San Francisco	May 31-Jun 4	www.ncore.ou.edu
Diversity @50 (AARP Diversity and Inclusion Conference)	Baltimore	Jun 13-14	www.aarp.org/about-aarp/events/diversity50
11th Annual International Conference on Diversity in Organizations, Communities and Nations	Cape Town, South Africa	Jun 20-22	www.ondiversity.com/conference-2011
AAAA Access, Equity and Diversity 2011 Summit and Annual	Atlantic City, NJ	Jun 28-30	

FOR MORE INFORMATION ON CYBERFOR'S DIVERSITY PROGRAM CONTACT:
LCDR CHRISTINE COCHRAN AT (757) 492-8827 X 2 OR CHRISTINE.COCHRAN@NAVY.MIL

DIVERSITY SPOTLIGHT



Mrs. Virginia Grizzle

(Left) Virginia Grizzle is assigned to NETWARCOM and has been a council member since 2008. Virginia served as a Flag Coordinator and now assists with the Diversity Awards board. She also facilitates the Appreciating Differences seminar.

(Right) CTMCS(SW) Samantha Blackwell works in N43 with the Navy's Cryptologic Carry-On Program. She has been involved with NCF's Diversity program since checking on board in January 2010. Her most enjoyable time is serving as a mentor, assisting 7th graders at Churchland Middle School in the BIOBASE program. ✌



CTMCS(SW) Samantha Blackwell

DEPARTMENT OF THE NAVY

**Navy Cyber Forces
Public Affairs Office
2465 Guadalcanal Road STE 10
Virginia Beach, VA 23459-3243**

PRESORTED STANDARD

**U.S. POSTAGE PAID
SOUTHERN MD
PERMIT No. 1968**

Address Service Requested

Official Business

