SHIPYARD LOG

Pearl Harbor Naval Shipyard & IMF News Since 1946

October 2018

An in-depth look into
Information Technology
@ PHNSY & IMF

Making IT Happen

CYBERSECURITY

Capt. Greg Burton, USN
47th Commander
Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility

Cybersecurity, Everyone's Responsibility

First, let me thank all those personnel who planned, participated, and executed the 'Ohana Day Picnic at Bellows Beach - Mahalo! It was a great day and great time for all who were able to attend and I think everybody was able to win something – there were enough prizes to go around. Code 200 won the Captain's Cup, with Code 930 a close second. I look forward to next year's 'Ohana Day and an even larger turnout.

Next, I wanted everyone to know that we entered this fiscal year with a signed budget (First time in a decade), which means that we will be able to execute our FY 19 plan without the normal funding reductions and the continuous re-racking of our funding phasing plan that has been our normal mode of operation in the past environment of Continuing Resolutions. Bottom line, we need to discipline ourselves to our execution strategy and perform to that plan. Since we haven't been in this financial environment for years, here are some things to think about. We need to aggressively obligate funding such that we will have an 80% obligation rate by 31 Jul 2019. What does that mean in more detail? It means a couple of things. There is no reason to delay our hiring actions to later in the year – we need to hire to the plan. Every effort needs to be made to increase the number of people on the deckplates, versus just working more overtime with fewer people; overtime will be high in the first quarter of this fiscal year due to our high workload. Also, with Direct and Indirect Non-Labor, understand the requirements, the phasing and execute to the plan. One more note, look for opportunities to award our employees earlier in the year for the great things that they are doing to accomplish our mission.

This month we are focusing on Cybersecurity. This is an area of our mission that is not as easy to comprehend or visualize, like delivering a submarine back to the fleet, but nevertheless, a vital part of our mission here in Pearl Harbor. Cybersecurity is one of Naval Sea Systems Command's (NAVSEA) major themes in the "Expand the Advantage" Campaign Plan and we directly support this priority. As we know, the entire world is connected through the internet and other electronic means. At the same time, our adversaries our operating relentlessly to deny, disrupt, disable, and damage our critical networks. The Navy must keep their networks secure from attacks. NAVSEA has charged Pearl Harbor Naval Shipyard and Intermediate Industrial Facility with protecting our networks both afloat and ashore (e.g., machinery control, combat system control and ashore-based information technology) from both insider and external threats. Our Information Technology & Cybersecurity Office, Code 109, plays a key role in this mission accomplishment, as does each on of us.

The objectives of this NAVSEA Mission Priority are 1) Increase our level of knowledge of threats, processes and procedures to support the fleet, 2) Affordably integrate cybersecurity in our products, and 3) Execute our responsibilities within the new Risk Management Framework. Success in this priority is realized as we prevent, detect, characterize, and mitigate cyber-attacks on our shipboard and shore networks.

Our (Code 109) staff put together for this issue some interesting articles covering an overview of our network operations as well as pertinent topics that touch on our day-to-day activities at work and that align to NAVSEA's campaign plan. Topics such as technical operations, support services, innovation, and strategic planning. Also included is a discussion of cyber warfare and regulation adherence that informs us of the need to remain vigilant at work and at home. Our level of Cybersecurity is only as strong as our weakest link. Together we can strengthen our cyber defenses.

Last but not least, let's remember the Navy's Birthday this month - 243 on 13 Oct this year!

October 2018
Vol. 71, Number 10
https://www.flickr.com/photos/phnsy/

Commander
Capt. Greg Burton

Public Affairs Officer
John Whitehouse

Editor
Justice Vannatta

Commander's Comment Line
474-4729

Fraud, Waste & Abuse Hotlines
Shipyard Hotline
471-0555
NAVSEA Hotline
(800) 356-8464
Navy Hotline
(800) 522-3451
DoD Hotline
(800) 424-9098

Safety Hotline
471-8349

Report-to-Work Status Hotline
473-9000

SHIPYARD LOG: This DoD publication is authorized for members of the Shipyard. Contents of the Shipyard Log are not necessarily the official views of, or endorsed by, the U.S. government, DoD, or PHNSY&IMF. ISSN 1073-8258.

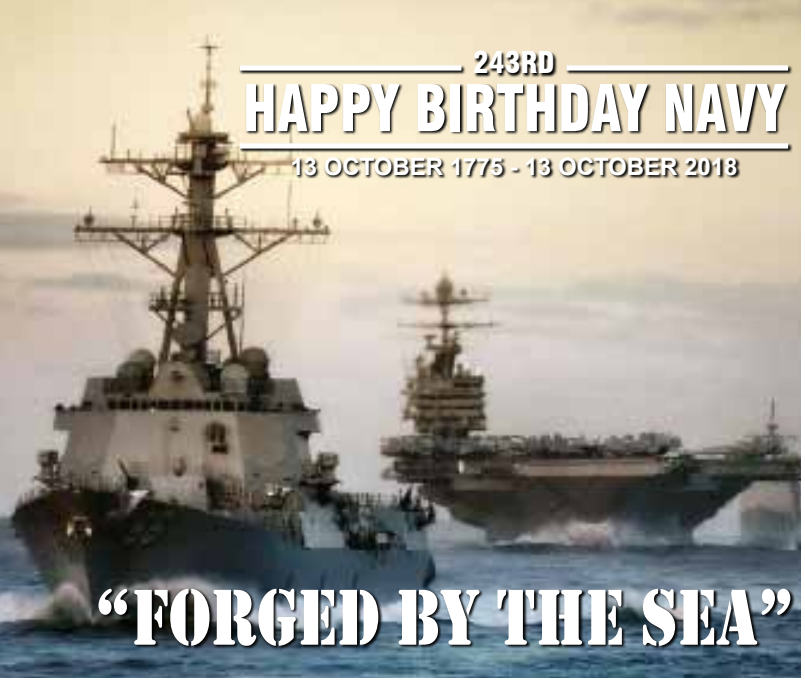
PUBLICATION DATES: The Shipyard Log is published monthly. Articles are due the 10th of each month. Send material to the editor via email or, if hard copy (typed, upper/lower case) on a CD via inter-office mail to Code 1160 Shipyard Log. All material is subject to editing.

MAILING ADDRESS:
Shipyard Log Editor
PHNSY & IMF (Code 1160)
667 Safeguard St Ste 100
JBPHH, HI 96860-5033

CONTACT INFO
Telephone: (808) 473-8000 ext. 4157
Fax: (808) 474-0269
Email: Justice.vannatta@navy.mil

ON THE COVER:
C109.31 IT Specialist Laarni Endozo

Graphic art by: Dave Amodo
Photos by: Justice Vannatta



Happy 243rd Birthday US Navy!!

Story courtesy of Navy.Mil

In an effort to curb British Sea Control, the Continental Congress established the Continental Navy, which later, on October 13, 1775, became the United States Navy. When the Navy was first formed, it consisted of just two armed vessels – tasked with disrupting munition ships supplying the British Army in America. Yet over the past nearly two and one-half centuries, our Navy has grown to become the largest, most advanced, and most lethal fighting force the world has ever known.

In 1972, the Chief of Naval Operations, Admiral Elmo Zumwalt, designated October 13 as the Navy's official birthday, and directed that it be commemorated so as to "enhance [the] appreciation of our Navy heritage" and reinforce "pride and professionalism in the Naval Service."

The theme for the Navy's 243nd Birthday is "Forged by the Sea." Our commemoration of the Navy's birthday offers us an opportunity to honor the brave men and women who conduct a wide range of combat, training, humanitarian, rescue, and other missions worldwide, protecting the nation's interests, promoting its security, and helping to shape our history and culture.

Since its earliest days, the U.S. Navy has deployed forward to deter our adversaries and to fight and win in the event deterrence fails. In today's increasingly complex global security environment, the Navy continues to provide forward presence in areas where our nation's interests are being challenged, including the Arabian Gulf, South and East China Seas, Red Sea, North Atlantic and beyond.

As our adversaries, both actual and potential, strive to match and outpace the capabilities of our fleet, it is imperative that our Navy continue to grow, develop, and innovate to maintain maritime superiority. A reflection on the Navy's 243 years of sea power offers an ideal opportunity to strengthen our national resolve in that direction.

Photo by Dave Amodo

USS Chicago (SSN 721) Successfully Undocks

Story by Blythe Goya Public Affairs Office

On September 10, Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility (PHNSY & IMF) successfully undocked the Los Angeles-class fast attack submarine, USS Chicago (SSN 721), from Dry Dock #3.

The ship's force, project and undocking team worked together to accomplish an expedited major emergency diesel overhaul, first of its kind, in the middle of anticipating severe weather conditions. "Great job to the undocking team, for planning, coordinating, and executing a safe undocking - in the midst of preparation for inclement weather," expressed Project Superintendent CDR Dave McGlone. "Also, great job to all for readying the pier for USS Chicago with all temporary services in just 24 hours, a record turnaround time."

Repairs to USS Chicago also include a complete external hydraulics system flush. This major modernization package is considered a substantially larger work package than the notional package to support a service life extension, providing more operational time to the fleet. "The size and complexity of this Docking Selected Restricted Availability (DSRA) is unlike any other," said McGlone. "Every member of the project team with the support of the entire shipyard, expertly removed barriers to complete this challenging 10-month docking period, ultimately leading to a safe execution of the most complex type of undocking evolution at PHNSY&IMF."

Chicago is the fourth ship of the United States Navy to be named for the city of Chicago, Illinois. After completing a two-year maintenance and upgrade period at PHNSY in October 2011, Chicago arrived in April 2012 at her new homeport, assigned to Submarine Squadron 15, based at Joint Region Marianas, Naval Base Guam. The submarine is 362-feet long, displaces 6,162 tons, and is equipped to carry Mark 48 Advanced Capability (ADCAP) torpedoes and Tomahawk land attack missiles.

Campaign Plan To Expand The Advantage

Story & photos by Justice Vannatta
Shipyard Log Editor

"The price of freedom is eternal vigilance."

- Thomas Jefferson, third President of the United States of America, circa1801

Cybersecurity is the theme of this month's *Shipyard Log*, in recognition of National Cybersecurity Month. NAVSEA's ***Campaign Plan to Expand the Advantage*** emphasizes that each and every NAVSEA employee bears the responsibility to better understand cybersecurity and the role we each play in supporting the fleet and keeping our systems safe. To ensure we remain ahead of our nation's adversaries, we must establish a culture that embraces cybersecurity awareness and compliance, and use high velocity learning to reach that goal.

"Our ships and systems are increasingly dependent on electronic data and information systems to operate, communicate, and deliver essential services," said NAVSEA Commander, Vice Adm. Tom Moore. "In our daily jobs, we are also dependent on computers, networks, and information systems. One of the fastest ways to lose our advantage is for our adversaries to deny, disrupt, disable, or cause physical damage to our forces and infrastructure through electronic attacks. That is why Cybersecurity remains both a challenge and warfighting imperative for the U.S. Navy. Individually and collectively, we need to establish and practice sound cybersecurity habits. We must also integrate Cybersecurity into every facet of our business to protect, detect, react, and restore our systems from cyberattacks."

During a recent visit to Pearl Harbor Naval Shipyard & Intermediate Maintenance Facility, Vice Adm. Moore addresses the entire workforce, thanking the personnel for their dedication, tenacity and hard work.

The brightest American minds and most strategic tacticians are needed to protect from terrorist threats against the United States. The FBI's Internet Tip Line, which handles both terrorism and domestic crime reports, has received an average of more than 700 messages/day since it was set up after Sept. 11, 2001. That number does not come close to representing the total number of tips the government receives, since many leads come from people walking into U.S. embassies, pulling aside police officers, or contacting state and local hotlines. Counterterrorism analysts deal with a staggering volume of information which includes not only direct tips, but also wire intercepts and leads from paid informants. National Counterterrorism Center director Michael Leiter says that when you add all that up, the agency receives between 8,000 and 10,000 pieces of information per day, identifying as many different people as potential threats. The Center also learns about an average of 40 projected plots daily against the United States or its allies. This number does not include cybersecurity threats.

Cyberattacks on America are an ever-increasing security threat. The FBI reports that since Jan. 1, 2016, more than 4,000 ransomware attacks (a type of malicious crypto-virology software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid) – happen daily. That's a 300 percent increase from 2015, when the daily average was 1,000 attacks. Americans polled last month by Pew Research identified cyberattacks as the second greatest global threat to the U.S., behind ISIS (Islamic State of Iraq and Syria). A new report by the Government Accountability Office (GAO) also reveals how the cybersecurity threat has grown. In a survey of 24 federal agencies, the GAO found that between 2006 and 2016, the number of cyberattacks climbed 1,300 percent – from 5,500 to more than 79,000 per year. There is a global war going on, and a global arms race to go with it. The arms race is not a race for physical weapons; it is a race to develop cyber-weapons for psychological, emotional, financial and infrastructure attacks. A cyber weapon is a tool that is used, or designed to be used, with the aim of threatening or causing physical, functional or mental harm to structures, systems or living things.

Many experts predict that World War III will initially begin with massive cyber-attacks. According to a former national

NAVSEA Commander Vice Adm. Moore discusses the importance of workload management, utilizing resources and fostering a culture of affordability with former Commanding Officer Cmdr. Kevin Moller, USS Jefferson City (SSN 759).

security advisor, Dr. Paul D. Miller (National Security Council Staff), a future world war would break out in gradual stages – beginning with cyber and anti-satellite tactics by the aggressor nation(s) to take down much of the world's communications infrastructure. Miller's comments come as North Korea has been blamed by the international community for the "WannaCry" cyber-attack last year which crippled the United Kingdom's National Health Service (NHS) as well as other government departments and organizations around the world. Meanwhile, Russia has been accused of colluding in the 2016 U.S. presidential election and the alleged hacking other governments' systems – claims Moscow has repeatedly denied.

Cybersecurity is everyone's responsibility. It is up to each of us to get educated on cybersecurity and understand that the threats to our country and our allies are real. We need to understand that one simple act of irresponsibility and oversight is all the enemy needs to gain an advantage that instantly puts lives at stake. Our eternal vigilance is required not only to defend our state and nation, but also to ensure the survival of the modern world as we know it.

Code 300 Zone Manager Collin Chun shares information with Vice Adm.Moore on the innovative mock-up of the stern planes and rudder of a 688 class Submarine. The mock-up has fully functional moving parts and may be disassembled as necessary. Shop 38's Steering & Diving Core Team utilizes the 3D printed mock-up when training apprentices, during workability meetings, and in pre-job briefs.

Ohana Day Picnic 2018

Story and photos by Jason Okumura

Code 109.1 Technical Support Division Head

Blue skies and trade winds described another fun filled day at the Annual Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility (PHNSY & IMF) Ohana Picnic. Festivities started early on the morning of Saturday September 22 at Bellows Air Force Base beach on the east side of Oahu. Mahalo to PHNSY & IMF's Morale, Welfare, and Recreation Committee for putting together another awesome event and to the Federal Manager's Association for distributing the delicious bentos.

Hundreds of shipyard employees and sailors attended the annual event with their family and friends participating in various activities such as the water balloon toss, donut eating contest, trivia, and keiki fun activities. Door prizes this year included a flat screen TV, iPad, Go Pro cameras and for the grand prize, an outer island trip for two.

Congratulations to Code 200 for being crowned this year's Captain's Cup winner. Prior to the picnic, team sporting events were held in dodgeball, basketball, flag football, bowling, and billiards. The final events of volleyball and a relay race were held during the picnic to determine this year's winner. Going into the final event, there was a tie for second place between Code 930 and Code 2300 that was settled with a tiebreaker relay race resulting in Code 930 as second place and Code 2300 as third place overall in the Captain's Cup standing.

Collaborative Teaming Creates A Strong Cyber-Defense Posture And Reliable IT Services

Story by Randy Chang
Code 109 Activity Command Information Officer

Code 109 Cyber Security Specialists Virgil Brewer, Code 109.1 Division Head Jason Okumura Code 109. 3 Division Head Darwin Uesato, Code 109 Activity Command Information Officer Randy Chang, Code 109.2 Division Head Marci Watanabe, Cyber Security Specialists Matthew Wong and Anthony Logie.

Collective Learning Through
Information Sharing

When information systems that process data are depended on for advancing critical work, producing metric data points, and driving work decisions, it is imperative that greater information sharing about past and present threat incidents and data-breaches help organizations stay ahead of threat actors, social engineering attempts, and their tactics. Cyber tools for detection, data analytics, threat response, and data recovery are improving, however, staying close knit with each other in what's happening in our shipyard as well as the experiences we encounter outside of our shipyard help to vector down areas in information technology (IT) & cyber security where improvements can be made before it becomes an unacceptable risk to operations. Facilitating information sharing can be enforced by a policy driven approach, through forums such as the cyber security working group, the department Information Assurance Officer (IAO) briefings, or community driven information sharing learning cells. These examples allow organizations to learn from a collective pool of past and present cyber experiences and helps us gain knowledge of how we can protect ourselves and our IT systems from attackers and bad actors.

Team Defense
Must Be Played As A Team

Cyber security is a team sport and it takes an informed group of stakeholders to address cyber risk. All of us play a pivotal role in managing cyber risks alongside a well-trained team of IT professionals who understand what is not right in our daily digital processing and how to effectively address these anomalies. The more we learn and share amongst ourselves about our digital world, we build a better team defense to keep our ships and personnel Fit to Fight.

Driving Forward
The Digital Transformation Agenda

Embedding processes, developing expertise and tools to deal with risks associated with new digital projects ensures that organizations develop cyber resiliency, transforming to embed digital solutions within our core business of keeping our Navy safe. Leading the charge in innovative solutions is a strong cyber security core that outlines the boundaries and identifies the risk impacts to our Navy networks. As we collaborate together to deliver viable and effective digital solutions, a strong partnership of learning and understanding about what is in the realm of possibilities is a solution for success.

Tech Ops to Cyber Ops Journey

Story by Jason Okumura
Code 109.1 Technical Support Division Head

Over the years, Information Technology (IT) has evolved and become more complex. We've gone through waves of centralized processing (Honeywell mainframe) to distributed computing (personal computers/stand-alones). We are now in a hybrid of technologies that span both central processing and distributed computing, which is further complicated by the multiple environments (i.e., NMCI, SYLAN, SECNET, etc.) that we use. Through the increased connectivity of technologies, there has been an exponential increase in cyber-attacks. Our department is now named the Information Technology and Cyber Security (ITACS) Office as cyber security is integrated into our technical operations.

We manage traditional IT technologies (i.e., servers, storage, networks, and applications), but we have implemented multiple technological advancements and deployed various cyber security tools to improve the performance of our systems and meet regulatory requirements.

On the server & storage front, we've implemented server blade technologies, virtualization, terminal services, and centralized storage. These technologies have reduced our server footprint, improved system performance, increased fault tolerance and redundancy, configuration controls, and energy conservation.

Our network team has been vigorously working on modernizing our network infrastructure in conjunction with the dynamic moves on the waterfront in addition to implementing new network technologies such as next generation firewalls, network intrusion and prevention systems, virtual private networks, and device authentication technologies that contribute to our layered Computer Network Defense (CND) strategy. The network team also manages our Voice and Video over Internet Protocol (VVoIP) system that provides critical communication for the shipyard.

Corporate Applications are the bread and butter of our ship maintenance community. We manage our corporate applications, Department of the Navy applications, and web-based collaboration tools. This includes application release management, financial fiscal year rollover and cutover, and a variety of solutions such as specialized database query and reporting functions.

Our shipyard has a classified Secure Network (SECNET) that is an extension of the larger Naval Nuclear Propulsion Program Network (NNPP Net). We have a SECNET Team to ensure the IT needs of our nuclear community are being addressed. This team encompasses the full spectrum of IT capabilities including servers, storage, network, CND, Helpdesk, and applications. Project availabilities rely heavily on this team to provide timely IT Temporary Services needed during project execution.

The future of the ITACS Office holds many opportunities. Our servers and storage capacity will be refreshed to ensure we leverage technological advancements to optimize our system performance and meet regulatory compliance. We will continue to modernize our network infrastructure and expand our wireless coverage in addition to improving the VVoIP capability to an enterprise Unified Communication (UC) solution. Evaluation of the Internet of Things (IoT) will be needed as we move forward with network enabled equipment and smart devices. Some of our systems will need to be managed remotely as we migrate our corporate applications to the centrally hosted Maritime Systems Environment (MSE), which will also include Electronic Technical Working Document (eTWD) capability. MSE is projected to eventually move to cloud services under the Navy Maritime Maintenance Enterprise Solution - Technical Refresh (NMMES-TR) initiative. We will be continually evaluating our cyber defense strategies and incorporate more sophisticated tools that leverage event correlation, analytics, artificial intelligence, heuristics, and behavioral analysis techniques.

Front row: C109.31 IT Specialists Kam Ng, C109.31 IT Specialist Valerie "Leilani" Loredo, C109.31 Supervisor IT Specialist Suzan Wagatsuma, C109.31 IT Specialist Laarni Endozo, C109.31 IT Specialist Kiley Kaneshiro.
Back row: C109.31 IT Specialist Ralph Bolabola, C109.31 IT Specialist Alan Domingo, C109.31 IT Specialist Devin DeTurk and C109.31 IT Specialist Jung-Hoon "Christian" Choi.

Information Technology and Cyber Security (ITACS) Customer Advocates

Story by Darwin Uesato, IT Strategies & Client Services Division Head

Need a computer? Phone? NMCI account and email? Software, access to an application, webpage, file share folder? Maybe a monitor, printer or multi-function device? Or simply having a bad information technology (IT) day, making it hard for you to help our shipyard deliver ships Fit to Fight!!

The IT and Cyber Security (ITACS) Customer Advocate Program is being developed to engage Code 109 into key shipyard business areas, with a focus on non-stop execution of critical chain work by the mechanic on the deckplate and helping solve significant shipyard problems. Currently, ITACS Customer Advocates are involved and building relationships Project Teams on the waterfront; providing dedicated support to Code 105.6 ECC, as well as Code 900T Production Training. The Network Operations Security Command Center (NOSCC) is an innovative, proactive approach to perform continuous monitoring of ITACS from a holistic perspective to "give minutes back to the mechanic on the deckplate" by defending the cyber security tenets of Confidentiality, Integrity, Availability, Non-Repudiation and Authentication; and to Expand the Advantage Mission Priority of Cyber Security. The End-Device Management Branch is being established to dedicate ITACS expertise to IT-enabled shipyard equipment and innovation, also known as Platform IT or Unconventional IT – in collaboration with end-users, such as, production shop equipment mechanics.

This customer-focused program involves building two-way relationships, where Code 109 is integrated with shipyard business priorities, processes and requirements, and in return, shipyard business areas are empowered with knowledge of ITACS services, capabilities and cyber security requirements to protect our military data and information systems. The desired outcome of the program is to continuously develop the capability of predicting ITACS needs, and be ready to deliver secure services and solutions when and where ITACS is needed.

Customer advocacy is a combination of customer relationship management, which is knowing what IT and cyber security services and solutions the shipyard needs and when they are needed, and customer experience, which is delivering secure IT services and solutions with the intended value, meaning, high quality service with satisfied customers. In layman terms, creating and maintaining customer relationships, understanding customer needs, and providing services to meet those needs while maintaining acceptable risks to cyberspace, including DoD systems, at the same time.

The ITACS Office is a customer service organization. The role of Code 109 as representatives focused on IT maintenance and security will change. A renewed focus on customer experience and delivery of ITACS services that impact shipyard mission will be the defining feature of the next wave of business innovation. Rather than Code 109 passively processing requests for IT services, the future will be more about IT collaborating with customers to proactively provide IT solutions and capabilities that result in increased productive capacity for the shipyard. Poor customer service is no longer acceptable. This realization will change the way organizations behave in regards to ITACS, as well as change the level of service expectations in its new role.

To gain credibility as a customer-focused organization, mental models must be broken. Cyber security must be a strong enabler for innovation, vice inhibitor. Business decisions must be made with strong ITACS knowledge and experience upfront, vice perceived as a constraint after decisions are made. Organizational changes have been made to foster this culture change. Code 109 reports directly to the Commanding Officer; is a member of the Shipyard's Senior Leadership Team; and shipyard senior leaders are actively taking ownership and providing leadership for ITACS issues.

We must establish a culture that embraces cyber security awareness and compliance, and applies high velocity learning to ensure we remain ahead of our adversaries, with a focus on culture of affordability and innovation, that results in on-time delivery of ships and submarines.

Imagine a future when ITACS will be collaborative and engaged, with a customer-focus and a digital transformation agenda, delivering secure IT services and solutions where and when IT is needed to help O.U.R. shipyard keep ships Fit to Fight!

The IT Strategies & Client Services Division is the primary starting and ending point in the customer experience.

- Front desk support is provided by the IT Customer Support Branch at Building 1916, and manages the IT Service Management ticket system where requests are submitted.
- The IT Planning & Admin Branch plans and executes the IT budget and procurements to deliver IT hardware, software and contracts needed in our shipyard.
- The IT Solutions Branch manages the shipyard intranet and SharePoint websites and local databases that automate workflows, provide on-line collaboration workspaces and process data where legacy corporate applications may not meet our shipyard's needs.
- The End-Device Management Branch manages end-devices, such as desktops, laptops, and tablets, primarily on our shipyard network as well as stand-alone workstations.
- The OCONUS Program Manager delivers IT services and solutions to locations outside of our Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility campus.

Cyberspace: The 5th Domain

Story by Marci Watanabe
Code 109.2 Information Assurance Division Head

Cyberspace… is the newest of the 5 DoD Operational Domains (i.e., Maritime, Land, Air, Space, and Cyberspace). The pace at which technology over the Internet has moved is unprecedented, as evidenced through the use and reliance of our mobile devices. This makes the access to information very easy for us… and the bad guys. With our dependence and convenience of these tools comes everyone's responsibility to safeguard personal and government information. Information Technology (IT) is often the only weapons system commands like the Shipyard has to help defend our nation.

The Command Information Systems Security Manager (ISSM) is a role that all federal organizations must have. While an important method to keep the nation safe, is through the compliance with rules and regulations, at the Shipyard we focus on developing relationships via the ISSM's Philosophy of: *To Build Shared Commitment Rather than to Force Compliance.*

The Shipyard's ability to remain resilient in cyberspace relies on a number of programs such as:

1. Department Information Assurance Officer (Dept. IAO)
2. Cyber Security Working Group (CSWG)
3. IT Grams

Related information can be found at: https://phportal.phnsy.sy/code/C109/Pages/Home.aspx.

Department Information Assurance Officer (IAO)

Each department has a Department Information Assurance Officer (Dept. IAO). The Dept. IAO may have a support team of Alternate Information Assurance Officer (AIAO), Terminal Area Security Officer(s) (TASO), and Alternate Terminal Area Security Officers (ATASO). The Dept. IAO, AIAO, TASO and ATASOs are the liaisons between your department/code/shop, and Code 109 for IT issues. This includes assisting with and enforcing compliance in areas of cyber security such as: account validation, proper handling/disposition/destruction of media, incidents, vulnerabilities, and IT asset moves.

Code 109 holds Dept. IAO meetings every other month to increase awareness and communication on Code 109 solutions and issues such as: the latest cyber security policies; how to get services from Code 109; recent cyber threats and incidents; and updated guidelines for networks, hardware, and software. Documents such as meeting presentations are located on the Department IAO Portal.

Cyber Security Working Group

PHNSY & IMF has commissioned a Cyber Security Working Group (CSWG) sponsored by the Shipyard Commander to increase the survivability of the Command's mission in a cyber-warfare environment through assessment, action, and knowledge sharing. The CSWG provides advice and guidance on cyber security to the shipyard community, and assists in the application of cyber security best practices through Code 109's Department IAO program and Senior Leadership Team (SLT). The CSWG aids in the management of IT risks to computer systems and business by performing risk assessment, business impact analysis, and maintaining a Shipyard-wide unconventional IT inventory to improve management, identify trends, make predictions, and safeguard assets. Documents such as illustrations of cyber security compromise are located on the Department IAO Portal.

One of the events coordinated by the CSWG was the NAVSEA partnership with the National Security Agency (NSA) to provide training and demonstrate proper use of NSA protective technologies. The purpose of the visit was to educate the shipyard community on the current threat landscape the US Navy is faced with today's environment, and potential security risks pertaining to Standalone IT systems. Three skilled experts from NSA demonstrated techniques to protect industrial/computer systems through the use of protective technologies, such as port (USB, RJ45) blockers, cable locks and tamper evidence labels. The NSA site visit was a success due to the outpour of support from CSWG and subject matter experts from various functional codes along with the Public Affairs Office.

IT Grams

Code 109 also issues IT Grams as a tool to continuously increase shipyard awareness of IT solutions and issues, including communicating what's going on, who's who, what we do, and what is expected of shipyard employees to help bridge the gap between IT and shipyard business. Recent articles include: NMCI Operating System Upgrade, Antivirus and Microsoft Home Use Programs, Cyber Security in the Workplace is Everyone's Business, and SECNET Helpdesk Open Hours.

The most current IT Gram is the annual special edition for National Cyber Security Awareness Month (NCSAM). October is NCSAM, and the 15th year of the U.S. Department of Homeland Security's annual campaign to raise awareness about the importance of cyber security. NCSAM educates the public and private sector partners about the importance of Cyber Security, provides them with tools needed to stay safe online, and increases the resiliency of the Nation in the event of a cyber-incident. This and other IT Grams are located on the Code 109 homepage.

In Focus:
Info Technology

C109.12 Network Administrators Vince Tabata and Scott Matsuda with their Network Branch Manager Len Christensen review network topology diagrams.

Photos by Justice Vannatta

C109.34 System Administrator Ryan Kemp builds a workstation for shop equipment.

C109.34 System Administrator Craig Gentry with C930 Electric Technical Work Document (eTWD) Aaron Asato review tablet specifications and application performance on tablets.

C109.12 Infrastructure Specialist Lorin Chun interconnects cables between network cabinets.

Code 109 and Cyber Security

C109.11 System Administrator Victor Loui replaces server blade fans in the server farm to ensure proper cooling and fault tolerance.

C109.11 IT System Administrator Rachel Kiyabu reviews system logs to optimize operational performance and identify anomalous activity.

C109.31 Customer Support Devin DeTurk with ITSC(SS) Anthony F. Rossi III coordinates with ship force on establishing NMCI connectivity to the barge.

C109.11 IT Storage Administrator Adam Butac removes tapes used for backing up critical shipyard data for disaster recovery.

C109.12 Infrastructure Specialist Dan Endozo works on fiber connection for the Chicago Project Team.

CONGRATULATIONS!!

Safe Shop of the Month

Shop 98, Crane Maintenance

TO REPORT AN INCIDENT OF HARRASSMENT, CONTACT:

CODE 100CE DIRECTOR: 473-8000 x4355
CODE 100CE DEPUTY DIRECTOR: 473-8000 x6073

HOTLINE:808-474-4829

TO FILE AN EEO COMPLAINT, CONTACT: EEO OFFICE: 808-471-0241

Photo by Dave Amodo

June Service Awards

10 Years
Kelly Cripps, C290.2
Eaton Dayrellstulen, C300
Rinnah Israel, C610
Nicholas Jurasek, C2340
Thomas Kagawa Jr, C105.3
Dennis Ke, C246
Michael Knapp, C246
Christopher Lambert, C260.2
Dru Nakasone, C930
Christopher Peterson, C920
Clint Rodriguez, C960
Melvin Shinohara, C109.3
Dallon Sims, C970

20 Years
Brian Apo Jr, C740
Charles Kahana, C970
Todd A Miller, C2702
Kevin Owens, C990
Mose Tyrell, C930
Alfred Viloria, C920
Baron Yamamoto, C136.1

25 Years
Mary Garcia, C600
Michael Polesky, C930

30 Years
Gavin Adaro, C990
Alejandro Agtarap Jr, C2340
Warren Amaral, C244.2
Dean Arakaki, C1055
Rayvyn Boots, C300
Bonifacio Gabaylo Jr, C960
Garrick Goya, C950
Amy Kawamata, C950
Ryan Namaka, C900T
Fernando Nerona, C1055
Howard Shiroma, C1053
Alden Takaoka, 300N

35 Years
Bradford Costales, C2601A
Wilson Resurreccion, C990

40 Years
Joseph Baldauf III, C740
Allan Takamori, C1331
Mark Wong, C2305

45 Years
Carlton Chang, C930
Henry Dement, C900T
Ronald Ota, C990

Fair winds & following seas to June Retirees

Eric Desilva
Alphonse Godbout Jr
Roy Kobashigawa
James Lentz
Ferdinand Madriaga

June Civilian Newcomers

June McClendon C105.5
Zachary Mon C960
Andrew Montalbo Jr. C970
Scott Morisaki C970
Hiilani Morita C2320
Nicko Naanos C246
Joshua Navarro C106.3
Alyson Nishimura C109.3
Jason Ohara C981
Ronald James Pablo C105.5
Reagan Paz C2350
Joseph Christian Peralta C260
Justin Pham C2330
Atreyu Ragil C970
Robert Ramos C246
Desiree Razon C950
Jayson Reynon C105.5
Lenard Ruiz C2380
Wyatt Rushing C710
Aidan Delgado III C2340
Shannon Owens C900T
Nicholas Sumera C138
Enzo Takiguchi C990
Justin Tice C2340
Quentin Willis C2340
Christine Wipfli C105.2
Erin Yamamoto C2320
Christopher Young C246
Cody Allen, C960
William Anderson, C2205
Christopher Assily, C741
Arthur Banaticla, C742
Loreto Bartolome III, C950
Jacquelyn Bomar, C106.3
Tanya Buttner, C410
Iman Cababag, C270
Robin Caplett, C710
Kimberly Cavaco, C290
Brendan Chang, C250
Howard Chin, C138.2
Lorin Chun, C109.1
Michael Collins, C1121
Kuika Cordeira, C970
Barbara Darabos, C109.2
Armani De Ocampo, C930

June Military Newcomers

ETN1 Kevin Cariffe C990
LCDR Robert Fauci C103
MMN2 Joben Fernandez C300N
MMN1 Christopher Gomez C990
EN2 Keenan Kotanen C930
EN2 Haley Magnin C930
MMW2 Tyler Patterson C300
ITC Tuan Pham X-Div
MMN1 John Seay C990
FT1Bryan Seiber C305
EMN2 Brandt Shoech C246
MMN2 Michael Smith C930
BMCS Alvin Vinarao C760
FT1Brandon Washington C246
ETNC Stephen Wilson C950

Connect with the Shipyard on Facebook & Twitter / PearlHarborNavalShipyard