Security and Emergency Services Community of Interest Newsletter

Spring 2014

COI MISSION

The Security and Emergency Services (S/ES) Community of Interest (COI) creates professional development opportunities, provides community forums, and promotes the interests of Marine Corps S/ES organizations.

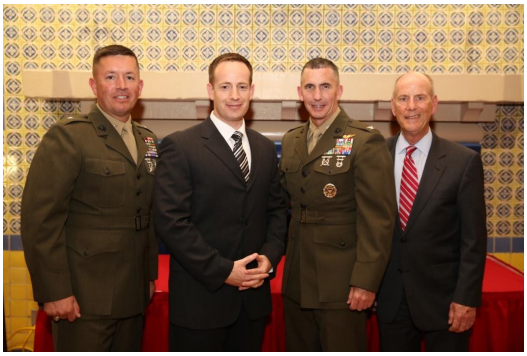
COI VISION

To become an essential partner with installations and operating forces by providing Security and Emergency Service members individual career development opportunities and a network for exchanging knowledge, improving communications, sharing best practices, and finding innovative solutions which will deliver improved organizational capabilities to meet future safety and security needs for Marines, civilians, and their families.

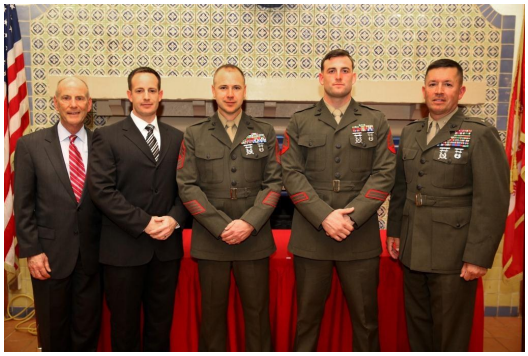
Inside this issue:

A Message from the Community Leader

Welcome to the Spring 2014 edition of the Security and Emergency Services Community of Interest newsletter. First, I'd like to congratulate Mr. Jude Gronenthal of the MCAS Miramar Provost Marshal's Office for his selection as the 2013 Civilian of the Year. This year was marked by the most submissions ever for this award; a testament not only to Jude's performance but also to the professionals of our community and their leaders' desire to recognize them. Jude was recognized in March at the annual Marine Corps Senior Leaders meeting in San Diego.



The 2014 Senior Leaders Security Meeting, MCRD San Diego CA, March 2014. From left to right – BGen James Bierman Jr., CG, MCRD San Diego/Western Recruiting Region, Mr. Jude Gronenthal, Provost Marshal's Office, MCAS Miramar, 2013 Civilian of the Year, Colonel John Farnam, Commanding Officer, MCAS Miramar, and Mr. Raymond Geoffroy, Assistant Deputy Commandant (Security), Plans, Policies, and Operations.



The 2014 Senior Leaders Security Meeting, MCRD San Diego CA, March 2014. From left to right - Mr. Raymond Geoffroy, Assistant Deputy Commandant (Security), Plans, Policies, and Operations, Mr. Jude Gronenthal, Provost Marshal's Office, MCAS Miramar, 2013 Civilian of the Year, MSgt John Alen, Marine Special Operations Group, Marine Corps Special Operations Command, 2013 Jim Kallstrom Leadership Award, Sgt Miles Jones-France, Marine Special Operations Team 8111, 1st Marine Special Operations Battalion, 2013 Jim Kallstrom Bravery Award, and BGen James Bierman Jr., CG, MCRD San Diego/Western Recruiting Region.

Second, I'd like to highlight a critical aspect of the Marine Corps' security program – the Continuous Evaluation Program. The Continuous Evaluation Program is designed to ensure individuals with security clearance eligibility are continually screened so that any information or actions that fall under specified adjudicative guidelines are immediately reported to the DoD Central Adjudication Facility (CAF). The CAF will then review the report to determine whether the individual will maintain their current clearance eligibility. Individuals who exhibit behavior that may indicate otherwise are a potential threat not only to national security but quite literally to the lives of others (e.g., the first Fort Hood shooting and the more recent Washington Navy Yard shooting - in both instances, the shooters exhibited behaviors that clearly should have been acted upon).

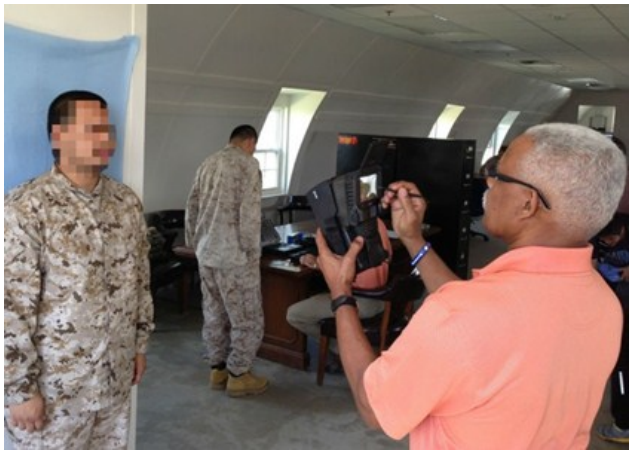
SECNAV Manual 5510.30 lays out the responsibilities of all hands concerning the program as well as a list of 13 behaviors or actions that should be reported/acted upon. It tasks commanding officers with establishing and administering the program. It further mandates that commanders, supervisors, managers, and coworkers report these behaviors and directs commands to report these behaviors without attempting to apply or consider any mitigating factors which may exist. These last requirements sometimes cause leaders to hesitate in reporting these behaviors – there may be a natural affinity to "protect" an individual or to avoid "embarrassing" the command by reporting such behavior. This mindset is unacceptable – it has literally led to the loss of life. I ask leaders at all levels to re-commit themselves to this program. Your local Security Manager can provide additional information.

Once again, thanks for all of your hard work and dedication to country and Corps.

Semper fidelis,
Raymond F. Geoffroy
Assistant Deputy Commandant (Security)
Plans, Policies, and Operations

The Gold Standard in Background Checks—Marine Corps Role Player Vetting

by Mr. Nick Hall, HQMC, PP&O (PSS)



Provost Marshal Office Quantico, PMO Services Officer, Mr. Reyes Gonzalez , administers the biometric collection portion of the RPTS Program enrollment.

(Photo by Nick Hall)

As of the first quarter of 2014, the Marines Corps is now pioneering a higher level standard in Antiterrorism/Force Protection (ATFP) screenings. With the recent incidents at Ft. Hood, the Navy Yard, and other installations, vetting thoroughly and to stringent standards is a cornerstone in Security and ATFP. Marines at bases all over the United States are beginning to receive new training on the Role Player Threat Screening (RPTS) Program. This program screens all Role Players the Marine Corps hires to support cultural and ethnic learning programs and other training, but screenings occur in a very unique way – with biometrics.

Biometrics is nothing new: the Federal Bureau of Investigation (FBI) has been using fingerprints since the 1920s, and for at least a decade, the Department of Defense (DoD) has maintained a fingerprint, face, and iris database that is used to identify terrorists. The RPTS Program incorporates biometrics into the contractor hiring and vetting process, but this too is nothing new. So what's the "Gold Standard"? Why so sensational with the article title? RPTS does several things exceptionally well: Biometrics are used to confirm the subject standing in front of you; Subject history is established; and continuous vetting occurs well after the subject leaves the base. The key is Biometric Continuous Vetting.

As learned from the 2013 Navy Yard incident, the perpetrator had all the proper contractor screenings; however, if continuous vetting had occurred, more recent police reports would have surfaced and helped to identify risks. This continuous vetting in RPTS is the difference and is being made possible by joint agreements between the FBI and Headquarters Marine Corps (HQMC). This program provides a national collaboration amongst bases with quality and current information. If a Marine Corps installation on the east coast bans an individual for misconduct, all bases nationwide are notified immediately. If a hired role player gets a felony arrest a month after working at MCB Pendleton, all participating MCBs will be notified. These notifications and records are bridging the gap when a civilian is banned from one base and attempts to apply to another.

In April, HQMC released a message (DTG 111752ZAPR2014) detailing this year's Mobile Training Team (MTT) base visit locations and dates. This will involve software updates, system refreshes, and state-of-the-art training on RPTS. With the combination of new biometric equipment, FBI and Naval Criminal Investigative Service (NCIS) support for continuous vetting and new United States Marine Corps (USMC) policy, Program Management Offices (PMOs) throughout the United States will not only lead the way in the Marine Corps, but will lead the way throughout the DoD as maintaining the highest standards ever implemented for hiring Role Player personnel.

Energy Security

by Mr. Doug Phelps, HQMC, PP&O (PSM)

The Mission Assurance Branch, Plans, Policies and Operations, in conjunction with the Deputy Commandant, Installations and Logistics and the Commanding General, Training and Education Command, is developing a strategy and implementation plan to support the assurance of secure, reliable and redundant sources of energy-primarily electric power-to support continued operations of significant missions, functions and supporting critical assets and infrastructures in the event of prolonged outages of commercially supplied electrical power.

There is significant Congressional and DoD focus on energy security, resiliency and sustainability. Section 335 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2009 requires the Secretary of Defense to "Conduct a comprehensive technical and operational risk assessment of the risks posed to DoD's mission critical installations, facilities, and activities by extended power outages resulting from failure of the commercial electrical supply or grid and related infrastructure."

Further strategic guidance is outlined in the 2014 Quadrennial Defense Review Report: "The Department has invested in energy efficiency, new technologies, and renewable energy sources to make us a stronger and more effective fighting force. Energy improvements enhance range, endurance, and agility, particularly in the future security environment where logistics may be constrained." Also, the NDAA provides facilities/installation guidance, to include requirements to address energy security while simultaneously enhancing mission assurance; and directs a coordinated energy assessment to prioritize critical assets and ensure that critical assets are prepared for prolonged outages (natural disasters, accidents, terrorist attacks).

ALMAR 011/11 (Marine Corps Expeditionary Energy Strategy), discusses increased use of renewable energy at installations and directs 50% of installations to be net-zero energy consumers by 2020. Per the ALMAR, "Changing the way we use energy is essential to preparing our Corps for the future…. Our vision is to be the premier self-sufficient expeditionary force, instilled with a warrior ethos that equates to efficient use of vital resources with increased combat effectiveness…." The Commandant has charged each Marine and civilian Marine to change the way we think about energy in leading, training and equipping our expeditionary force.

Two Energy Security Pilot Assessments have been conducted at Marine Air Ground Task Force (MAGTF) Training Command 29 Palms and Marine Corps Air Station (MCAS) Miramar. The goals of the Energy Security Pilot Assessment are to develop a standardized and repeatable methodology that identifies the specific missions and power requirements for facilities aboard installations. With this in mind, the data sets that are collected during these assessments will allow commanders at all levels to understand the importance of each facility, based on the mission and essential functions that facility supports. In the near future these data sets (Mission Dependency Index "MDI") can be used to support numerous prioritization efforts across Mission Assurance related projects within the Marine Corps. Some examples of the data the assessments collect are as follows: identify the average peak electricity loads each facility requires to sustain missions, core functions and essential operations; identify key electric nodes that support these facilities and can be potential single points of failure; identify key regional commercial electric generation and transmission nodes that support these facilities and can be potential single points of failure for the provision of commercially supplied electricity; identify and document current back-up capabilities, to include refueling plans and priorities, back-up generator capacity for fuel, maximum run time, and identifying and documenting estimated times that organizations can continue their missions and functions without the provision of electricity before the mission or function is significantly impacted. The endstate is to conduct standardized and repeatable Energy Security Assessments at all bases and installations.

Alerting the Corps to Imminent Threats and Hazards

by Mark Brown, Marine Corps Installations Command, G-3

The insider threat: At 1000, the disgruntled former government employee showed up at the base Human Resources (HR) office with gun in hand. Fortunately, he was more inclined to voice his grievances than to shoot, but within 10 minutes of his arrival, a Supply Sergeant's wife at the Commissary was alerted on her mobile phone to avoid the area of the building with the HR office. Simultaneously her husband's computer screen flashed a similar warning.

The weather hazard: The forecasters got the timing right for the oncoming storm, just not the intensity. It arrived right on time at 0300, dropping 6 inches of snow instead of 1 inch. The base Commanding Officer was alerted and the decision made to alert base personnel of a Code Blue late opening. Within minutes, emails and text messages arrived at the homes of base personnel, preventing many people from being on the roads before state road crews could clear the snow.

The HazMat hazard: At 1445 on a Friday afternoon, a tanker truck carrying a hazardous material (HazMat) was involved in an accident at the main entry to the installation's industrial area. Within minutes, the 2,500 civilian employees of the industrial facility received instructions via a computer pop-up alert, email, telephone voice message alert, outdoor Giant Voice, or Indoor Voice to either shelter-in-place OR to evacuate the facility using an alternate route based on their location and proximity to the accident.

What do these three very different fictitious scenarios all have in common? They are examples of the power of the Marine Corps Mass Notification System (MCMNS), a new emergency management tool administered by the Marine Corps Installations Command (MCICOM) G-3 Installation Protection (IP) Branch.

Since December 2013, all Marine Corps installations have had access to the MCMNS, a mass notification system intended to quickly notify users about emerging and emergency situations via computer screen pop-up, email, phone, text, and both indoor and outdoor public address system alerts.

"The MCMNS is an important component of the Marine Corps' Emergency Management Program, helping ensure the safety and security of personnel aboard our installations," said Mr. Thomas Ruffini, MCICOM G-3 IP Branch director. "In our technologically connected world, the MCMNS gives us the ability to reach users during an emergency which is critically important to our overall Installation Protection strategy." Fort Hood's use of its wide area mass notification system to alert personnel to immediately take shelter in response to the April 2, 2014 shootings, adds tragic credibility to Mr. Ruffini's remarks.

In the aftermath of the Fort Hood shooting in November 2009, the Secretary of Defense "commissioned the *DoD Independent Review Related to Fort Hood* to assist the Department in identifying existing gaps and deficiencies." One of the deficiencies noted was a lack of a robust mass notification system on DoD installations. The Independent Review panel recommended "deployment of state-of-the-art Mass Notification and Warning Systems (MNWS) and incorporate these technologies into emergency response plans. The purpose of MNWS is to provide warning and response direction for all personnel within 10 minutes of incident notification and verification. MNWS has four elements: (1) Giant Voice for outdoor areas; (2) Indoor Voice for indoor facilities; (3) Telephone Alert System for phone call/text alerts; and (4) Software Alert Systems for computer alerts."[1] DoD Instruction 6055.17, DoD Installation Emergency Management Program, subsequently mandated this MNWS standard for all DoD installations.

The Marine Corps already had Giant Voice on its installations, with Indoor Voice an element of new construction and many rehab projects. While some installations had a variant of the Telephone Alert System, the Marine Corps lacked a state-of-the-art Software Alert, or network-centric system. Early in 2010, Headquarters Marine Corps, Plans, Policies, and Operations, Security Division (HQMC PP&O (PS)) tasked Space and Naval and Warfare Command (SPAWAR) Systems Center – Atlantic (SSC LANT) Marine Corps Electronic Security Systems (MCESS) Group to determine available options for deploying a network-centric mass notification system for the Marine Corps.[2] Following a comprehensive review process, AtHoc, Inc., with its IWSAlerts system, was selected. In June 2013, an Authorization to Operate and Connect the MCMNS to the Marine Corps Enterprise Network (MCEN) was granted. A draft Concept of Operations (CONOPS) provided initial direction for the MCMNS. The official HQMC policy direction for use and support of the MCMNS is under development.

Alerting the Corps to Imminent Threats and Hazards Cont'd

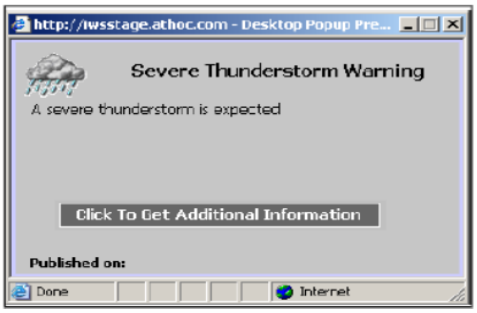
HQMC PP&O PS fielded AtHoc IWSAlerts and conducted operator and administrator training at all USMC installations, from September-December 2013. In December 2013, the system was turned over to MCICOM G-3 IP Branch to manage and administer.

Some installations have already used the MCMNS.

- Shortly after installation, the Marine Corps Mountain Warfare Training Center, Bridgeport, CA used the MCMNS to publish an Amber Alert. While this alert did not result in an apprehension or recovery of a child, it did demonstrate a valid use of the system.

- Marine Corps Base Quantico (MCBQ) quickly developed procedures to use the system. They implemented procedures to test the system daily and to improve operator proficiency. MCBQ has already used the system several times to notify its users about the impact of weather conditions this winter on base access. Col David W. Maxwell, MCBQ Commanding Officer, put it this way, "MCBQ developed internal procedures, exercised the system, and then implemented it as a key component of the distribution of command information and emergency notifications. Over the course of multiple snow emergencies this winter, we have employed the notification system with much success and it has proven to be a better product in ease of use and effectiveness of notification."

- Following the 8.2 magnitude earthquake that struck northern Chile on April 1, killing six people and triggering a small tsunami, Marine Corps Base Hawaii used its MCMNS to send this warning to its personnel, "STAY OUT OF THE OCEAN. STRONG UNDERCURRENTS ARE POSSIBLE. REMOVE BOATS FROM THE WATER, IF POSSIBLE."



While the initial fielding and implementation of the AtHoc IWSAlerts system was relatively smooth, there have been challenges with maintaining the underlying Information Technology (IT) infrastructure because the Marine Corps is transitioning from the existing network services contract for the Navy Marine Corps Intranet (NMCI)/Marine Corps Enterprise Network (MCEN) to the Next Generation Enterprise Network (NGEN) contract that provides the Marine Corps with greater control of its intranet infrastructure.

The simultaneous transfer and transition of the MCMNS program of record from PP&O PS to MCICOM G-3 IP Branch has created some IT support challenges for the ongoing functionality of the AtHoc IWSAlerts system. These issues are being addressed by a diverse group of subject matter experts (SMEs) from MCICOM and its subordinate regional MAGTF IT Support Centers (MITSC), as well as SMEs from the Marine Corps Network Operations and Security Command (MCNOSC), SSC LANT, NMCI support team and the vendor, AtHoc, Inc.

The MCMNS requires seven things to be effective:

1. It must be considered a life-safety system, just like a fire alarm. It must work continuously 24 hours a day, 365 days a year.

2. Operators need to know how to use the system to publish alerts. This requires initial training, but also subsequent follow-on training AND regular use of the system to maintain proficiency.

3. Contact information needs to be current in terms of phone numbers (work/personal) and email addresses. The system automatically pulls contact information from the Active Directory/Global Address List (GAL).

   End users, the personnel receiving alerts, must ensure that their information in the GAL is accurate. They are also given the opportunity to add family phone numbers to their personal profile so that family members can receive alerts. An agreement between HQMC and American Federation of Government Employees (AFGE) C240 allows collecting contact information from union employees.[3]

Alerting the Corps to Imminent Threats and Hazards Cont'd

4. Everyone on the installation needs to be educated on the system, i.e. what to expect when alerts are published, how they will be published and what people are expected to do when they receive alert warnings. At installations like MCB Quantico, where the MCMNS is being used regularly and effectively, initial education of end-users in addition to operators and administrators was a key first step.

5. The MCMNS needs to be a component of an installation's regular emergency management exercises to ensure it is working as expected and to further educate end users on how they will be notified. Judicious use of text messages and telephone alerts is important as those alerts carry additional fiscal costs.

6. The installation MCMNS requires developing clear and concise pre-scripted messages based on likely hazard scenarios the installation could encounter. Pre-written messages allow for the rapid and effective publication of alerts and warnings. Alerts and warnings need to be specific regarding:

    - The hazard or threat,
    - The area at risk,
    - The predicted time of impact,
    - The expected response actions.

    Several scripted alert scenarios are provided as part of the AtHoc IWSAlerts package. These scenarios can be customized to the needs of individual installations.

7. A well-established IT support system to ensure the system always functions the way it was designed. As noted earlier, efforts are underway to ensure this is in place.

The MCMNS is just one element of an installation's Emergency Public Information (EPI) function, which is a key component of emergency planning. People are less likely to panic if they know plans are in place and as a result they know what to expect AND what is expected of them. People will also seek to validate the alerts they receive through other people they know, i.e. via social media like Facebook or Twitter, so it is critical that all EPI alerts published by the installation is consistent in its messaging.

Adverse events will continue to impact Marine Corps installations, from severe weather to terrorist or insider threat incidents to technological emergencies. The MCMNS will help mitigate the effects of said events by reducing the number of casualties, injuries and damage to property. The MCMNS will positively improve the ability of Marine Corps installations to safeguard the personnel who come aboard every day to support the Operating Forces in completing their missions.

References

1. Secretary of Defense Memorandum: "Final Recommendations of the Ft. Hood Follow-on Review," August 18, 2010

2. Space and Naval Warfare Systems Center – Atlantic Report, "Report On Findings Electronic Alerting Mass Notification Systems," February, 2011

3. Memorandum of Agreement between HQMC and AFGE C240, Subj: ATHOC Mass Notification System, Dtd February 5, 2014

USMC Network Dependency — It is More than Access to the Internet

by LtCol Andrew Drake, HQMC Strategic Initiatives Group

The Challenge. Consider the following three separate events that occurred in 2013.

- A large Marine command lost Marine Corps Enterprise Network (MCEN) services usage for four days due to a malfunction that shut down power to its common infrastructure.
- A homeless man in Hawaii lit a fire underneath a viaduct that accidently burned some cables which interrupted much of Hawaii's communication backbone for at least 20 hours.
- A Marine command's ability to execute some basic functions (e.g., print, access local share drives, issue weapons, etc.,) was disrupted for seven hours after a burst steam pipe caused a loss of network connectivity which was then compounded when a networking device failed after the circuit was reenergized.

Undoubtedly, there were additional events last year that, while not as disruptive, were still serious and are indicative of the extent to which we are vulnerable to network outages.

The Concern. The aforementioned events all occurred at garrison locations and were the result of non-deliberate actions. Imagine the possibilities for a disruption to network access in an expeditionary environment when dealing with a threat employing deliberate kinetic and/or non-kinetic efforts against your network.

Although the issue of increasing dependence on technology has been haunting many for years, what may be the Corps' blind spot is limited awareness of the operational impact from a lack of network access; i.e., a full understanding of each unit or weapon system's limitation if the network is not available. When that limitation is understood, deliberate mitigating measures can be developed that could include: justification for appropriate budget allocation to harden the network; redundancy efforts to eliminate single points of failure; and maintaining a non-network dependent skill set.

Secretary of Defense Hagel stated on 24 February, 2014 that "…we are entering an era where American dominance on the seas, in the skies, and in space can no longer be taken for granted." This statement, describing our operational environment, should explicitly include that we are no longer able to rely on information dominance. Undoubtedly, DoD leadership recognize Sea Control and Air Superiority can no longer be assured due to advances in Anti-Access Area-Denial (A2AD) capabilities but what is not fully appreciated is the operational impact when there is a lack of Information Dominance. This vulnerability should force the question of how the U.S. will address our future risk tolerance for operational actions and decisions.

This concern is much wider than the loss of administrative, logistic and even intelligence-related computer access – which could be operationally decisive on its own. However, we now have weapons systems that assume some type of network connectivity. The Joint Strike Fighter has networked dependency imbedded into it, as the information aspect of the F-35 is often touted as one of the most significant aspects of this platform. The M777 Howitzer's digital fire control and GPS-guided munitions could be adversely impacted without a network. Various sophisticated command, control and communication systems are obviously reliant on a network and could all be compromised. A recent body of students and faculty at the Naval Postgraduate School (NPS) discussed the concept of the "link dependency" of the network to the mission – it is like a weapon system. There was clear recognition of a linkage, but it was thought that the network is only an enabler and lacked a defined operational effect and therefore difficult to defend as a "weapons platform." The predominant view amongst the NPS students was that the network was vital to reach the "line of departure" and therefore is better classified as a core capability. Certain cyber capabilities may have a more direct path to being identified as a weapon system, but that platform further highlights the dependency on the network being operational.

At the Marine Corps Expeditionary Warrior 14 (EW14) Service-level war game in February, when one of the cells was designing the components of a Combined Joint Task Force (CJTF), the idea of having Cyber as a functional component command on equal footing with the Joint Force Air Component Commander (JFACC), Joint Force Land Component Commander (JFLCC) and Joint Force Maritime Component Commander (JFMCC) was considered. The idea was ultimately discarded as it was too difficult

USMC Network Dependency—It is More than Access to the Internet Cont'd

to determine the manning, roles, mission and responsibility of a Joint Force Cyber Component Commander within that wargame. Nonetheless, it is becoming more common to recognize the joint force and the Marine Corps have a dependency on the network and the utility of cyber-space as inextricably linked to our ability to complete the mission. Although Cyber Command and Marine Corps Cyberspace Command (MARFORCYBER) have been activated, it appears their full integration into operational commands is still being explored. The role and relationship of the network and cyber for any command and operation is becoming more complicated all the way down to a small unit staff. As we continue to wrestle with cyber and the network, we must get the doctrine right: who "owns" cyber in a command (a case can be made for the G6, G2 and/or G3); network dependency has grown beyond the conventional communication concerns; and what are the "manual" backups when the network is down for any reason – a unit cannot afford to shut down until the network is back online. As a military force, we are beyond the beginnings of the inflection point regarding the relevance of the network to how we operate; however, the distribution of our resources does not appear to match this level of importance.

Conclusion. There is no denying the need for the Marine Corps to maximize its effectiveness and efficiency through the use of technology and the integration of existing and future capabilities. As leaders, we need to ensure that we are aware of these changes and the inherent opportunity and risks this growing capability provides. As we move forward making the difficult choices inherent within a declining budget, we need to ensure there is an understanding of the importance and role network dependency has on current and future operations so that we can protect these critical capabilities and resources. Budget aspects aside, the Marine Corps needs to understand how it is dependent on the network in order to mitigate the risk, structure the force and develop the operational concepts to best pursue mission accomplishment.

Of note, when the communications went down in Hawaii, an investment banker stated "I quickly realized our service was down so I ran home and grabbed my laptop" because his company had a backup private network that they could revert to and rely on. Having a "Plan B" should be an imperative for the Marine Corps.

Around the Community:
Emergency Management Command and Coordination Success

by Ms. Jennifer Boughton, HQMC, PP&O(PSM)

Recently, the criticality of the ability to communicate between first responders and dispatch centers was highlighted. In the article, *Marines receive awards for emergency response to fatal accident on Okinawa highway*, a traffic accident was called in via radio to the Camp S. D. Butler 911 dispatch center enabling a much faster response by Military Police Officers.

The Land Mobile Radio (LMR) system for First Responders serves as a vital component of Okinawa's Emergency Management Command and Coordination (EMC2) program. The system provides a wireless capability for all DoD Services and offers superior flexibility during emergencies, significantly increasing collaboration efforts and interoperability. In certain parts of Okinawa, the terrain limits the coverage of wireless technology, but due to the shared LMR solution, users have the added benefit of seamless roaming into other Services' coverage areas. Fortunately, the Marines benefited from the availability of this first-class technology and were at the right place at the right time to support this unfortunate accident.

In the summer of 2008, communication planners throughout Okinawa came together and formed a grassroots working group. The parties met once a month, and continue to do so, to collaborate on each Service's focus areas and discuss ways ahead. The working group developed a cost sharing, operational and maintenance model to provide an affordable and practical method to manage and sustain a complex network of integrated communications equipment. The joint collaborative environment allows all LMR users, regardless of Service, to use the system which provides communication throughout Okinawa by leveraging the economy of force of all Okinawa installations requiring LMR service.

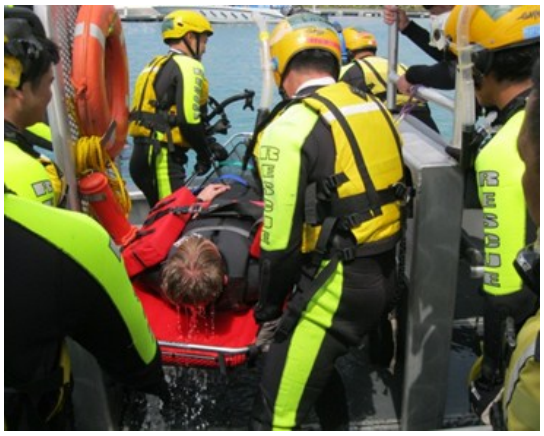
A full reprint of the article can be found here: www.okinawa.marines.mil/News/NewsArticleDisplay/tabid/18973 Article/160912/marines-receive-awards-for-emergency-response-to-fatal-accident-on-okinawa-high.aspx

Around the Community:

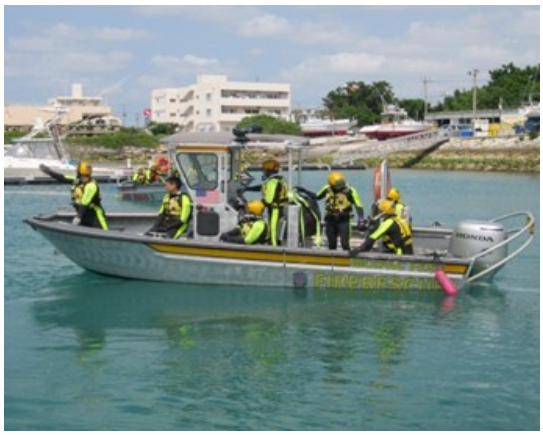
Marine Corps Installations Pacific Fire & Emergency Services Japan Ocean Rescue Training

by Frank Jones, Assistant Fire Chief, Camp Foster, JA

With the completion of the 2014 class for Ocean Rescue International Rescue Swimmer and Rescue Boat Operator, Marine Corps Installations Pacific Fire & Emergency Services Japan has increased its qualified water rescue personnel by 50 percent. This year presented some unusual challenges in the form of cooler than normal water temperatures. The beginning of the class on March 10th provided ocean temperatures of 68 degrees Fahrenheit, cool for those acclimatized to Okinawa, Japan. The lead instructor for the training was Joe Mokry from Ocean Rescue International whose credentials include; Instructor Trainer and Course Director - NAUI, EMTNR, US Coast Guard Captain License (100 ton) and US Coast Guard certified instructor - Fast Rescue Boats, and Personal Survival. This year the assistant instructor was Matt Novellino, a member of the U.S. Army Reserve, Special Forces and a former US Coast Guard rescue swimmer who served during Hurricane Katrina rescue efforts. The training consisted of areas including rescue techniques for panicked swimmers and the use of rescue paddle boards, jet ski assisted rescues, and rescues employing the department's rescue boats.



Rain occurred and nighttime swimmer navigation was included in this year's course. Rescue techniques involving rigging and conditions of fast water were also covered. The duties and responsibilities of coxswain and crew were instructed during the boat operator portion of the class. During portions of the training, the participants experienced on shore breakers of up to six feet with winds of 15 knots, gusting to 25 knots; all the while members of the teams practiced the rescue of swimmers from shoreline rocks and seawalls.



The valuable experience gained by the boat operators in maintaining boat position and safety during rescue operations are vital for real world events. Upon completion of the training, students received certifications of continuing education through the Maine Maritime Academy for Rescue Swimmer and Rescue Boat Operator.

Maine Maritime Academy is one of six maritime training colleges in the United States, and one of only two that fields a Navy Reserve Officers Training Corps (NROTC) unit. Ocean Rescue International's training met or exceeded all NFPA 1670 – Standard on Operations and Training for Technical Search and Rescue Incidents requirements for Technician level and the Public Safety Rescue Swimmer training program is the same program that is approved by the US Department of Homeland Security and the Federal Emergency Management Agency (FEMA). The entire course was not an easy one, but will provide benefits for years to come and the teamwork that was displayed and learned during the training will help build confidence; not only on water related events, but on all other events faced by the fire department's personnel in the future.

Around the Community:

Marine Corps Installations Pacific Fire & Emergency Services Japan Assist with Kuma Shima Triathalon

by James Hartman, Assistant Fire Chief, Camp Butler, JA

MCIPAC Fire & Emergency Service Japan (FESJ) firefighters recently volunteered their time and life-saving skills for the 2013 Kume Shima Triathlon on Kume Island near Okinawa, Japan. This past June, 15 water rescue specialists from Marine Corps Bases Japan Water Rescue Program on Okinawa and one member of the Torii Station Fire Department were requested by the organizers of the triathlon to provide water rescue support for the 240 participants in this year's event.

MCIPAC FESJ firefighters volunteered their own time to support this event and to positively represent the fire department for this premier event on Kume Island. This effort required the firefighters to arrange for travel and to transport their equipment to Kume Island, which lies 102 km southwest of the main island of Okinawa.

During the event, the MCIPAC firefighters were credited with assisting six of the participants in the water who experienced difficulties resulting from body temperature issues to muscle cramping. The fire department volunteers were able to assist the triathletes in the water and escort them safely to shore and render aid without further incident.

The MCIPAC Fire & Emergency Services Water Rescue Program is a program that started in 2006 and is a means to provide for surf and ocean rescue for the SOFA and Untied States Military personnel on Okinawa, Japan. This program consists of levels from lifeguard certifications to the licensing and use of water rescue craft in the form of boats, jet skis, and paddle boards. In the eight years it has been in existence, the program has responded to many calls for help and those calls have resulted in the safe return of persons in distress from the waters around the island.

ASIS Foundation/Military Liaison Council Certification Scholarship

by Staff Sergeant Chris Isely, HQMC, PP&O(PSS)

The ASIS International Military Liaison Council (MLC) is proud to announce that the 2014 ASIS Foundation/Military Liaison Council Certification Scholarship application period will run from May 13 to June 24, 2014. This scholarship recognizes outstanding ASIS active duty military members for their duty performance, community leadership, and self-improvement achievements and to assist them in advancing their career by achieving ASIS board certification. The scholarship awards funding to cover direct expenses associated with preparing for and achieving an ASIS board certification (Certified Protection Professional, Professional Certified Investigator, or Physical Security Professional).

All applications must be submitted directly to the ASIS Foundation staff (ASIS Foundation, 1625 Prince Street, Alexandria, VA 22314). Application packages will include the following:

a. Completion of the scholarship application form.
b. Cover/nomination letter signed by the military member's unit/organizational commanding officer or staff director. The cover/nomination letter should highlight nominated individual's mission/duty accomplishments, self-improvement efforts, and community involvement/leadership. The letter should not exceed two pages in length and must be written in English.
c. An essay completed by the nominated individual covering why they are pursuing a professional certification. The essay should not exceed one double-spaced typed page. It should be written in a 12-point, "Arial" or "Times New Roman" font. The essay must be written in English.
d. ASIS certification application for the certification for which they are applying.

ELIGIBILTY: Active duty military personnel assigned to the armed forces of any nation, who are ASIS members in good standing, are eligible for this scholarship. Additionally, applicants must meet the qualification criteria for the particular certification for which they are applying.

Application packages must be received by the ASIS Foundation no later than close of business on June 24, 2014.

A scholarship selection committee of MLC members will select ASIS military members for this scholarship. ASIS military members that apply for this scholarship and are selected will receive mentorship by the MLC through the certification process to ensure their success. Scholarship recipients will be announced/recognized at the ASIS Annual Seminar's Law Enforcement/Military Appreciation Luncheon in October 2014.

More information on the ASIS Foundation/Military Liaison Council Scholarship program can be found on the ASIS website at https://www.asisfoundation.org/Scholarships-and-Awards/Scholarships/Foundation-Military-Liaison-Council-Certification/Pages/default.aspx

CALENDAR OF UPCOMING EVENTS

ASIS Foundation MLC Scholarship Deadline no later than close of business on June 24, 2014

Register Now for Tuition Free Education Classes

by Ms. Jill Baker, HQMC, PP&O (PSS)

The Center for Development of Security Excellence (CDSE) Education Division offers courses designed specifically to develop leaders for the DoD security community. These courses are similar in scope to college and graduate level courses and are a semester long. Courses are delivered using a collaborative online learning environment, making them available to U.S. military members and government employees worldwide. No tuition or fees are required to take CDSE courses; however, some courses require the purchase of textbooks.

All of the courses have received college credit recommendations from the American Council on Education College Credit Recommendation Service (ACE CREDIT). Go to http://www.cdse.edu/catalog/elearning for a list of education courses.

To register, please log into STEPP via https://stepp.dss.mil/SelfRegistration/Login.aspx. If you have any questions, or need additional information, contact the CDSE Education Division at cdse.education@dss.mil.

Security Training

by Ms. Jill Baker, HQMC, PP&O (PSS)

Take advantage of free security training at http://www.cdse.edu/catalog/index.html. CDSE provides security education and training to DoD security program professionals, DoD contractors, employees of other Federal agencies and selected foreign governments. These courses are valuable to your security billet; useful for turnovers and on-the-job training. Training is available in multiple ways: instructor-led, webinars, e-learning, curricula, shorts, and virtual instructor-led.

Courses by Discipline

- Counterintelligence
- Cybersecurity
- General Security
- Industrial Security
- Information Security
- International Security
- Operations Security
- Personnel Security
- Physical Security
- Sensitive Compartmented Information
- Special Access Programs

Message Board

This section is designed to list messages of interest to the S/ES COI. All messages can be found on the S/ES SharePoint site at: https://ehqmc.usmc.mil/org/ppo/PS/SES-COI/default.aspx.

If you don't have an ehqmc account, you can establish one by contacting Mr. Billy Goard, the site's administrator, at billy.goard.ctr@usmc.mil.

Important Messages

MarAdmin 071-14 – CY 2013 Jim Kallstrom Awards Results
Maradmin 176-14 – Interim Guidance for Privately Owned Firearms Aboard Marine Corps Installations
CMC 081800Z Apr 14 – After Action Report 2014 Senior Leaders Training Event
CMC 111752Z Apr 14 – Marine Corps Role Player Threat and Screening Program MTT Visit Agenda
CMC 081418Z May 14 – Recouping Law Enforcement Flat Badges
COMMARSYSCOM 151849Z Apr 14 – Handling Instructions for Obsolete Controlled Cryptographic Items (CCI)