OVERWATCH

"The advancement and diffusion of knowledge is the only guardian of true liberty."
-James Madison

THE JOURNAL OF THE MARINE CORPS INTELLIGENCE OVERSIGHT DIVISION

Volume 8 Issue 2 Spring 2019

Photo by Senior Airman Sadie Colbert

IN THIS ISSUE, FEATURED ARTICLE: AT A CROSSROADS, NO MORE SHADOWS, THE FUTURE OF INTELLIGENCE OVERSIGHT IN CONGRESS

Inspector General of the Marine Corps

The Inspector General of the Marine Corps (IGMC) will promote Marine Corps combat readiness, institutional integrity, effectiveness, discipline, and credibility through impartial and independent inspections, assessments, inquiries, investigations, teaching, and training.

The Intelligence Oversight Division

To ensure the effective implementation of Marine Corps-wide oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and Special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Contact Information

Mail:

Director, Intelligence Oversight
Inspector General of the Marine Corps
Headquarters U.S. Marine Corps
701 South Courthouse Road
Building 12, Suite 1J165
Arlington, VA 22204

Intelligence Oversight Division Staff

GS15 Edwin T. Vogt, Director
Maj Greg Stroh, Deputy Director
LtCol Greg Ryan, Sensitive Activities Officer

Inside This Issue

3 **A Message from the Director**

4 **At a Crossroads, No More Shadows: The Future of Intelligence Oversight in Congress**

9 **Marine Corps Enhances Forensics Capability to Make Gathering Data Simple**

10 **Deactivation Ceremony Spurs New Beginning for Marine Corps GEOINT Training**

11 **Intelligence Photographs in the News**

Web Links

Senior Intelligence Oversight Official (SIOO)
http://dodsioo.defense.gov/

Marine Corps Inspector General
http://www.hqmc.marines.mil/igmc/UnitHome.aspx

Naval Inspector General
http://www.ig.navy.mil/

A Message From the Director

This edition of *Overwatch* is the second of calendar year 2019. It marks my 15th year in my position and I continue to be impressed with the caliber of individuals that our community attracts. As always, the articles provided in this issue do not represent the opinion of Intelligence Oversight Division or the Inspector General's Office. Instead, the articles are provided for information and awareness regarding current issues facing the community.

The first article in this issue was written by Mr. Tommy Ross. Mr. Ross is a senior associate at the Center for Strategic and International Studies. He also served as Deputy Assistant Secretary of Defense for Security Cooperation at the Pentagon and was the senior defense and intelligence adviser to Senator Harry Reid. This article is part two of a three part series titled *At a Crossroads.* This series provides a sweeping overview of the challenges the oversight community face.

Kaitlin Kelly from the Marine Corps System's Command Public Affairs Office provides the next article titled *Marine Corps Enhances Forensic Capability to Make Gathering Data Simple.* This article highlights a new and improved technology that is available to the MAGTF, Law Enforcement Battalions, and Marine Corps intelligence professionals.

Lastly, we here from the National Geospatial-Intelligence Agency, and the news regarding the deactivation of the Marine Corps Detachment at Ft. Belvoir, Virginia. Marine Corps geospatial intelligence professionals have trained at Ft. Belvoir since 1972. The detachment is relocating to Dam Neck, Virginia.

Semper Fidelis,

Edwin T. Vogt
Director, Intelligence Oversight Division
Office of the Inspector General of the Marine Corps
Ph: 703-604-4518 DSN: 664-4518 Email: Edwin.Vogt@usmc.mil

Featured Article

At a Crossroads: No More Shadows: The Future of Intelligence Oversight in Congress

Tommy Ross
War on the Rocks.com
May 16, 2018

In the 2012 James Bond film *Skyfall*, M (Judi Dench) and Gareth Mallory (Ralph Fiennes) debate how to respond to a leak that has led to the assassination of several MI6 intelligence agents. They are torn between a desire to ensure that MI6, Britain's premier spy agency, remains a credible part of British democratic institutions and the need to avoid antiquation in the face of rapidly changing technology and spycraft. At one point, Mallory laments, "We can't keep working in the shadows. There are no more shadows!"

Mallory and M's conversation encapsulates the broader, real-life dilemma that the intelligence community and intelligence oversight face in the modern era. Today, carefully guarded covert operations, undercover identities, and secrets of spy tradecraft can be exposed in seconds. Intelligence agencies face unprecedented political accusations of bias from their commander-in-chief. The tide of politics crashes headlong against the buttoned-up traditions of analytical integrity and inviolable protection of sources and methods.

There are indeed fewer and fewer shadows in which to conduct, manage, and oversee traditional intelligence work. Nowhere in Congress has that fact been more acutely felt than on the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, which oversee the organizations and activities of the U.S. intelligence community.

Over the years, congressional oversight of the intelligence community has wrestled with the balance between support and oversight, the extent of member and staff access to intelligence information, the challenge of transparency in a highly classified enterprise, and how to approach appropriating intelligence funding. The 9/11 Commission's 2003 Final Report described congressional intelligence oversight as "dysfunctional" – lacking "power, influence, and sustained capability." Committees in the House and Senate have different jurisdictions, different relationships with other national security committees, and different approaches to addressing intelligence community funding. Moreover, they do not have their own correlate appropriations subcomitttees the way the foreign affairs and defense committees do.

In part two of this series on national security oversight (read part one here), I argue that intelligence oversight is also at a crossroads. Existing challenges have been exacerbated significantly, but not exclusively, by the proclivities of the Trump administration, its openly adversarial relationship with the intelligence community, and congressional intelligence committees' high-profile investigation of Russia's interference in the 2016 presidential election. Intelligence oversight has also been challenged by the dizzying speed of modern media coupled with regular public leaks of massive amounts of digitized classified information, each of which increasingly intrudes on the shadows in which intelligence professionals are accustomed to operating.

Other factors – enormous growth of the intelligence enterprise since the 9/11 terrorist attacks, the technical complexity of many intelligence activities, and intelligence operations' prominent role in broader foreign policy – have left congressional intelligence oversight disadvantaged and struggling to keep up. But Congress must evolve along with intelligence, improving its capacity to confront these challenges, organizing itself for the mission, and developing new tools for new problems.

A Unique Oversight Role, Challenged

In many ways, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence share the same duties as all other oversight committees in Congress. They must ensure that the 17 agencies of the intelligence community have the personnel and resources to do

their jobs, are following the law, and are implementing policies in an appropriate and strategic manner. The committees hold hearings, write letters, conduct investigations, and pass legislation. But they diverge from other committees in one critical regard: Most of their oversight work is done in the shadows, in classified form and outside of public view.

The significance of this difference cannot be overstated. Other committees are also at the vanguard of oversight in their jurisdictions, but their work is buttressed much more robustly by public watchdog groups, lobbyists, think tanks, journalists, and even concerned private citizens. Although transparency on the other national security committees is not perfect, the policies they are considering are usually openly debated and dissected.

For the intelligence community, however, congressional oversight committees are the last line of defense. Beyond a small number of inspectors general and occasional reviews by the Government Accountability Office, there are no other entities with the access and mandate to check executive branch excess or error.

Most years, Congress passes a rather banal unclassified Intelligence Authorization Act, but the real meat of oversight legislation is contained in a classified annex to the bill. The annex is technically not law, but it is treated as such by the intelligence agencies who receive it, and they cannot discuss its details publicly. The vast majority of members of Congress are never exposed to the annex or to the intelligence community's workings more generally, so the burden falls on a small group of members and staffers to ask the right questions and sustain oversight initiatives.

Adding to the secrecy challenge, the already small intelligence committee staffs are divided and fractured: Only a subset of staff may have access to information on sensitive National Security Agency activities, while a different subset may be granted access to certain CIA information. This means that the congressional staff empowered to conduct oversight on any given issue often number in the single digits. And the defense appropriations subcommittees, which oversee the intelligence community's budget, do similar work with even smaller staffs than the authorizing committees.

Further, intelligence oversight committees must often negotiate – not always successfully – for access to vital intelligence with the very agencies they are charged with overseeing. Congress has three general levels of access to information at escalating levels of classification: the general membership, the intelligence oversight committees, and the "Gang of Eight" consisting of the top Republican and Democratic lawmakers in the House and Senate and on the two intelligence committees along with their corresponding staffs. Yet, the executive branch often makes unilateral decisions about which groups to share what with — sometimes information is given to only the Gang of Eight plus appropriators, for example, or to committee members but not staff. No clear rules guide these determinations, and key oversight staff are often excluded.

A third challenge is staff capacity. I can attest that the members and staff on the intelligence committees approach their unique oversight role with great rigor, seriousness, and patriotism. Quality bipartisan oversight on taxpayers' behalf goes on every day, though it rarely makes headlines. Yet the staff are snowed under by volume and complexity. Consider that intelligence committee staff must oversee and maintain requisite expertise on 17 separate agencies conducting intelligence collection and analysis through six major technical disciplines, while also maintaining specialized expertise to support oversight of research and acquisition programs and regional expertise to support oversight of intelligence strategies across high-priority countries and conflicts. As technological innovations in data analysis, artificial intelligence, cyber tools, and satellites grow ever more sophisticated, this complexity only increases.

According to the Congressional Research Service, intelligence committees have approximately the same number of staff now as they did in 1987. In that same period, five intelligence agencies have been created — not to mention the paradigm-shifting technological developments, particularly in space and cyberspace that have fundamentally changed and exponentially expanded technical intelligence collection. The intelligence community's budget, at over $70 billion,

is 18,421 times larger than that of the House Permanent Select Committee on Intelligence budget of $3.8 million. The inability of intelligence oversight committees to keep pace with the sprawling growth of intelligence agencies, personnel, and contractors is cause for concern, given the committees' role as the last line of defense.

In addition to problems of capacity and resources, the environment for intelligence activities is dramatically more public and more partisan than when the committees were first formed. Congressional staff lack the necessary tools and support to face the chaotic environment created by the enormous scrutiny of the tweet-driven media and partisan political groups on serious matters such as the Russia investigation. For example, despite the swirl of press inquiries about this probe, neither House nor Senate intelligence committees maintain any dedicated staff for media relations. Moreover, the challenge of conducting such high-profile investigations while protecting classified information and privileged discussions can erode the integrity of the oversight. The stumbling of the House intelligence committee's Russia inquiry as headed by its chairman, Devin Nunes, serves as a case in point.

In fact, investigations pose their own unique challenge to intelligence oversight. While investigations are typically viewed as special, occasional events, in practice, they have become an ongoing feature of intelligence oversight – a shift that staffing should reflect. In the past ten years, intelligence committees have conducted multi-year, detailed investigations of pre-Iraq War intelligence, the CIA's use of enhanced interrogation techniques, the 2012 Benghazi attacks, and Russia's election interference.

The time needed to complete a thorough oversight investigation does not comport with ravenous expectations of the political and media environment. Intelligence committees have faced considerable pressure to accelerate these politically sensitive reviews to keep up with the fast-paced news cycle. Such press interest has gone hand-in-hand with frequent leaks of intelligence secrets through actors ranging from Edward Snowden to the Shadow Brokers. Without dedicated investigative staff, each major leak that requires investigation diverts attention from normal oversight activities.

Another challenge is the cross-jurisdictional nature of many sensitive intelligence activities. Military intelligence operations, electronic surveillance programs, embassy management of covert action programs, and cybersecurity all cross into multiple committee jurisdictions. Moreover, the jurisdictions of House and Senate intelligence committees are not aligned. Gaps and redundancies in committee jurisdictions can create opportunities for the executive branch to evade oversight or venue-shop and can cause confusion and inefficiencies for overseers. Take, for instance, overseas collection of imagery intelligence: The Armed Services Committees must make determinations about resources for airborne intelligence, surveillance, and reconnaissance platforms without any knowledge of how the intelligence community's satellite programs might duplicate airborne collection. This breeds inefficiency and waste. While, on the House and Senate Appropriations Committees, a single subcommittee maintains oversight of both defense and intelligence enterprises, the subcommittee staffs are too small to effectively bridge this oversight gap.

Finally, oversight committees have always occupied the dual role of overseers of the intelligence community and explainers of its activities to the broader public. In recent months, the committees have been called upon like never before to serve as interpreters and even arbiters of attacks against the intelligence community from the president's Twitter account and, sometimes, from the media. However, this education function is of enduring importance. In the last two decades, there have been frequent controversies over intelligence activities, budgets, and authorities, but the public has had few tools with which to make sense of these debates. The dangers of a wide gap between intelligence activities and public information was demonstrated by the reaction to Snowden's leaks: Public opposition forced the termination of collection activities that the government had viewed as essential to counterterrorism efforts and that Congress had lawfully authorized and carefully (but secretly) scrutinized. The episode shows that the intelligence

community can no longer continue to operate strictly in the shadows.

Opportunity in the Light

How can the intelligence committees improve their oversight capabilities in an age where government secrecy has become increasingly fluid and, in some cases, an active target for attack? I propose several concrete measures.

First, intelligence oversight committees should pay much more attention to programmatic and organizational concerns, particularly through ongoing hearings. By its nature, real oversight lacks glamor, especially when almost no one knows what you are doing. Intelligence committee members get little political or constituent credit for delving into, say, the finer details of compartmented space programs or the way the CIA organizes itself bureaucratically.

Yet, the most mundane aspects of intelligence work – how agencies are organized, how personnel are recruited and developed, how programs are administered and executed, and how resources are budgeted and allocated – are the most important for effective oversight. Based on my own experience and conversations with oversight staff, however, the committees rarely conduct hearings dedicated to oversight of these issues beyond routine budget hearings, and few committee members invest in familiarizing themselves with their details. It is worth remembering that the 9/11 Commission overwhelmingly impugned bureaucratic issues – stovepiped communications, divided management, poor prioritization – not tradecraft, as the leading culprits for that intelligence failure. Avoiding such problems in the future requires careful, sustained oversight of the intelligence community's organizational structures, processes, and incentives.

Just as importantly, the committees should hold more hearings specifically dedicated to bureaucratic oversight, as opposed to specific threats or operations. A good place to start would be a sustained examination of the state of intelligence community integration after the reorganization brought by the *Intelligence Reform and Terrorism Prevention Act of 2004*. To my knowledge, this reform has received negligible attention from intelligence committees in the 14 years since its passage, despite the enduring importance of cross-agency collaboration and communication.

Second, as the House and Senate Russia investigations have painfully demonstrated, authorizing committees should maintain professional, nonpartisan investigative staff. Although the staff members handling high-profile investigations are highly competent, this work often comes on top of their daily support roles for their members and traditional oversight portfolios. Effective investigations require special expertise and rigorous attention. The committees should rebuild their bipartisan investigations teams and be resourced to do so with permanent, professional, nonpartisan investigative staffs who have the expertise to support future investigations.

Third, the intelligence committees must reshape their role as educators of the public. One way this can be done is by scheduling regular unclassified hearings that focus on the organization, personnel, diversity, and long-term resourcing needs of the intelligence community. House overseers have embraced public hearings far more than their Senate counterparts, but their open hearings have tended to focus on security threats rather than structural issues. Public hearings focused on the latter would do much to help the public understand the enduring national security importance of a robust, apolitical cadre of intelligence community personnel. In addition to public hearings, oversight committees should consider providing public notice of the general topics and, if appropriate, witnesses for their classified hearings, after consulting with the intelligence community on possible counterintelligence risks.

Fourth, the committees must create mechanisms to address cross-jurisdictional concerns in collaboration with other national security committees, the Armed Services and Judiciary Committees in particular. In my previous position, I witnessed regular competition and occasional suspicion among these committees on certain sensitive classified programs. Each panel has compelling reasons to think access should be expanded or limited. Shared defense and intelligence issues include oversight of special operations and the intelligence used to support them, targeted

counterterrorism strikes, and military intelligence operations. Meanwhile, both the intelligence and judiciary committees are invested in electronic surveillance and other issues involving intelligence support to law enforcement.

I'm not arguing for eliminating jurisdictional lines, but committees must figure out how to collaborate. They can conduct more joint oversight hearings, work with the executive branch to create stronger cross-committee access for certain members and staff, or even consider cross-committee task forces for sustained oversight challenges. Some progress was made on the access front in the Obama administration, but more needs to be done to create predictable and agreed-upon bipartisan, cross-committee oversight tools.

Fifth, the committees must address staffing challenges. More staff, including professional investigative staff, is certainly part of the answer. Though Congress is often averse to spending money on itself, it cannot expect the oversight committees to fulfill their responsibilities by keeping staffing levels flat while the intelligence community has doubled its size. But in addition, as others have suggested, the House Permanent Select Committee on Intelligence should follow its Senate counterpart's lead, enabling members to have cleared staff reporting directly to them and assigned to support their committee activities. These "designees" ensure that committee members have staff working to directly address their individual concerns and priorities as is the case with every other congressional committee. Intelligence oversight committees, which deal with increasingly sophisticated technical matters, would also benefit from the reestablishment of an independent technical support office, as proposed in Part I of this series.

Finally, Congress should negotiate or, if need be, legislate standard procedures for member and staff access to sensitive materials. Lawmakers should establish standard procedures based on the following principles. First, information should be shared on a need-to-know basis according to the responsibilities assigned each committee. Second, "Gang of Eight" notifications should be reserved for exceptional circumstances for the utmost sensitivity to national security. Third, at least for committees and the Gang of Eight, staff access should parallel member access. Fourth, for staff of oversight committees, the committees themselves should set access rules, rather than being subjected to arbitrary executive branch caps.

Conclusion

The last two decades have provided no shortage of cautionary tales about the risks of insufficient intelligence oversight. The 9/11 Commission found that "dysfunctional" oversight was a key contributor to the failure to prevent the 9/11 terror attacks. Intelligence committees failed to help Congress parse a distorted picture of Iraq's weapons of mass destruction programs, leading to a decade-long war costing thousands of American lives and hundreds of billions of dollars. In some cases, the executive branch deliberately stymied congressional oversight of the CIA's torture program. And Snowden's illegal disclosure of a vast trove of information about electronic surveillance not only damaged ongoing intelligence operations, but also convinced many citizens that they had been misled about the scope and intent of these efforts. As the shadows recede, it's obvious that challenges for effective intelligence oversight will only grow.

In *Skyfall*, when secretive intelligence operations are wrested from the shadows, people die. For once, real life is actually like the movies: Misguided intelligence operations, sloppy safeguarding of classified information, and bad policies put the lives of thousands of dedicated intelligence professionals at risk. Robust congressional oversight is the last line of defense against such outcomes. It is fitting, therefore, that later in the movie, Mallory, chairman of the parliament's Intelligence and Security Committee, saves M from an assassin's bullet. Despite institutional tensions and personal frustrations, legislative branch oversight remains the great shield of our democracy, and we must guard it vigilantly.

Marine Corps Enhances Forensics Capability to Make Gathering Data Simple

By Kaitlin Kelly
MCSC Office of Public Affairs
March 19, 2019

MARINE CORPS BASE QUANTICO, Va. -- The Marine Corps is enhancing an existing forensics exploitation capability used to differentiate between friend or foe on the battlefield.

The Corps is updating the Expeditionary Forensics Exploitation Capability, or EFEC, with newer IT technology. The EFEC is a portable forensic laboratory used by Law Enforcement Battalions to recognize, collect, analyze, preserve and store data.

The EFEC was fielded in 2013. Since then, the Identity Operations Team at Marine Corps Systems Command has decided to update the some of the system's IT equipment.

"We're making the IT equipment more adaptable for today," said Sarah Swift, Identity Operations Team Lead. "We're moving at the speed of relevance."

Maj. David Bain, EFEC project officer, believes employing more up-to-date equipment can benefit Marines on the battlefield.

"We want to improve the lethality of Marines in the battlespace by collecting and sharing data faster than we were previously able to," said Bain.

The EFEC is organic to the Marine Air-Ground Task Force and capable of exploiting forensic material to support forensically enabled intelligence. This includes device and digital media analysis, latent and patent print, DNA, and the collection and identification of other elements that can be forensically tied to activities.

The Identity Operations Team is working to integrate the EFEC with other intelligence systems to give Marines the ability to gain insight and information of immediate tactical value on the battlefield.

"EFEC complements and integrates with the other Identity Operations capabilities, such as Identity Dominance System-Marine Corps and the Marine Corps Intelligence Agency Identity Intelligence Analytical Cell, or MCIA I2AC," said Swift.

The MCIA I2AC reviews the IDS-MC and EFEC user's submissions and other collected data to provide direct support to the submitting Marines. The I2AC rapidly produces analysis reports and related products for persons of interest and shares this information, with the collected data, throughout the Defense Forensics and Biometrics Enterprise.

MCSC is assessing science and technology agile acquisition efforts now to develop and field the next increment of EFEC capabilities by fiscal year 2021.

"Marines want more expeditionary, rugged and lightweight equipment with fewer pieces, and we are making that happen with the EFEC," said Bain.

The Importance of EFEC

EFEC is a portable, expeditionary forensic exploitation laboratory that includes four collection kits. These kits provide squad-level tactical forensic collection capability for proper collection and preservation of evidence.

"The EFEC currently includes a chem kit, lab kit, media kit and site kit," said Bain. "Together, the kits enable Marine operators to gather important forensic information on site to determine if a person of interest is a suspect or an ally."

The chem kit allows operators to detect and identify hazardous and forensically relevant chemicals. The lab kit helps Marines process digital evidence, and the mobile kit helps to analyze and recover information from mobile devices.

Lastly, the site kit enables the operator to gather key forensic information, such as taking fingerprints and preserving liquids, at any location of interest.

MAGTF expeditionary forensics is one of three pillars within the USMC Identity Operations Strategy 2020 Implementation Plan. To fulfill the Marine Corps Operating Concept, MCSC continues to seek and provide Marines relevant, innovative and rapid solutions to enhance warfighting capabilities, Swift said.

"It's important that MCSC continues to advance with technology and we stay agile with our incremental acquisition approach to evolve current capabilities,"

said Swift. Matt Gonzales contributed to this story.

Deactivation Ceremony Spurs New Beginning for Marine Corps GEOINT Training

By Victoria Piccoli
National Geospatial Intelligence Agency
March 28, 2019

A Marine Corps detachment based at Fort Belvoir, Virginia, rolled and cased its colors during a deactivation ceremony March 26 at the National Geospatial-Intelligence Agency's campus in Springfield, Virginia.

The deactivation of Marine Detachment Fort Belvoir was part of a move to consolidate all Marine intelligence training at Marine Corps Intelligence Schools, a part of Marine Corps Detachment Dam Neck, Virginia Beach, Virginia.

Though the detachment at NGA was officially established in 2008, Marine Corps training in topography at Fort Belvoir began in 1972 under an NGA predecessor organization, the Defense Mapping Agency, said Nofziger.

While at NGA, the detachment successfully executed its mission over the years, said Nofziger. Over sixty Marines, served as instructors or support staff to graduate more than 1,300 geospatially-trained Marines.

The detachment's mission was to train and educate geographic intelligence, imagery analysis, and technical surveillance countermeasure specialists in their occupational field, said Marine Corps Capt. Nathan Nofziger, commander of Marine Corps Detachment at Fort Belvoir.

"These Marines will provide support to their commanders and the decision makers out in the field," said Phillip Chudoba, director of NGA's GEOINT Enterprise directorate. "We are going to miss you, but as members of the larger geospatial enterprise, you won't be too far."

The ceremony was paired with the last graduation of Marines at NGA, closing a chapter in Marine Corps history and the legacy of geospatial schooling at NGA. The next class of Marines training in geographic intelligence has begun at Marine Corps Detachment Dam Neck.

Intelligence Photographs in the News

U.S. Marine Corps GySgt David Friets with 3d Radio Battalion, III Marine Expeditionary Force Information Group attached to 3rd Marine Regiment, 3rd Marine Division launches a RQ-20 Puma Small Unmanned Aircraft System during Mountain Warfare Training 2-19 at Bridgeport, CA. Mar. 16, 2019. The Marine Corps Mountain Warfare Training Center provides Marines the opportunity to conduct tactical exercises in a cold weather environment, adapt and overcome snow terrain to continue military operations. (U.S. Marine Corps photo by Cpl Eric Tso.)

U.S. Marines with Fox Company, 2nd Battalion, 4th Marine Regiment, and 1st Intelligence Battalion, 1st Marine Division, survey a simulated attack zone during the Infantry Integration with Counterintelligence/Human Intelligence Operations (CI-HUMINT) (TACEX 19.2) at Marine Corps Base Camp Pendleton, California, March 21, 2019. TACEX 19.2 is an exercise for infantry and CI/HUMINT to tailor patrols for both units to effectively locate and sustain possible threats in order to properly train participants for combat deployments. Photo by LCpl Alexa Hernandez.

U.S. Marine Lance Cpl. Monique M. Szczepanski looks over mock terrain maps at Combat Town, Okinawa, Japan, Oct. 25, 2018. “I really love my job,” Szczepanski said. “I’m fairly new, so everything is a learning experience.” Szczepanski, a native of Johnson City, New York, is a geographic intelligence specialist with 3rd Intelligence Battalion, III Marine Expeditionary Force Information Group. 3rd Intel. Bn. is conducting the exercise to assess the abilities of their Marines in a field-like environment. (U.S. Marine Corps photo by LCpl Kevan Dunlop)

Intelligence Oversight Division

MISSION: To ensure the effective implementation of Marine Corps-wide Oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Examples of sensitive activities include:

- Military support to Civil Authorities
- Lethal support/training to non-USMC agencies
- CONUS off-base training
- Covered, clandestine, undercover activities
- Intelligence collection of information on U.S. persons

SECNAVINST 5430.57G states**:**

"...personnel bearing USMC IG credentials marked 'Intelligence Oversight/Unlimited Special Access' are certified for access to information and spaces dealing with intelligence and sensitive activities, compartmented and special access programs, and other restricted access programs in which DON participates. When performing oversight of such programs pursuant to Executive Order, they shall be presumed to have a 'need to know' for access to information and spaces concerning them."

WHAT IS INTELLIGENCE OVERSIGHT?

Intelligence Oversight ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories (*See References*).

DEFINITIONS

i. **INTELLIGENCE OVERSIGHT (IO):** Ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories. References: E.O. 12333, DoDM 5240.01, DoD Reg 5240.1-R, SECNAVINST 3820.3E, SECNAVINST 5000.34F, MCO 3800.2B

ii. **SENSITIVE ACTIVITY OVERSIGHT:** Any activity requiring special protection from disclosure which could embarrass compromise or threaten the DON. Any activity which, if not properly executed or administered, could raise issues of unlawful conduct, government ethics, or unusual danger to DON personnel or property. These activities may include support to civilian law enforcement. Reference: SECNAVINST 5000.34F

iii. **SPECIAL ACTIVITIES OVERSIGHT:** As defined by Executive Order 12333, activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies or media, and do not include diplomatic activities or the collection and production of intelligence or related support activities. Reference: **SECNAVINST 5000.34F**

iv. **SPECIAL ACCESS PROGRAM (SAP):** Any Program imposing need-to-know or access controls beyond those normally required for Confidential, Secret or Top Secret information. Such a program includes but is not limited to a special clearance, more stringent adjudication or investigation requirements; special designation of officials authorized to determine need-to-know; or special lists of persons determined to have a need-to-know. A special access program may be a sensitive activity.

v. **QUESTIONABLE ACTIVITIES:** Any conduct that may constitute a violation of applicable law, treaty, regulation or policy.