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 6 · Issue 1 · May 2017

Photo By: Lance Cpl. Ashley Phillips

IN THIS ISSUE: FEATURE ARTICLE – THE TEN PRINCIPLES OF INTELLIGENCE OVERSIGHT PROGRAM MANAGEMENT

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
VACANT, Deputy Director
LtCol Greg Ryan, Sensitive Activities Officer

Inside This Issue

Features

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/

Message from the Director, Intelligence Oversight

This edition of Overwatch is the first of calendar year 2017. It marks my 13th year in my position, and I continue to be impressed with the caliber of individuals that our community attracts. We need not look further than the recent general officer selection boards which included two intelligence professionals. Congratulations to Colonel Dimitri Henry who was recently selected for promotion to Brigadier General. Additionally BGen Michael Groen was selected to promotion to the rank of Major General. This is a credit to our community.

The first article in this issue was written by Mr. John P. Holland. Mr. Holland is a senior DoD official and a retired Army Military Intelligence officer. In his article for the Military Intelligence Professional Bulletin, Mr. Holland suggests 10 principles for a command's Intelligence Oversight program. Although focused on Army doctrine, his advice is sound, well-reasoned, and applicable to all services.

Sandra Jontz, of *Signal Magazine*, wrote our second article about an organization that will likely have a large impact on all of us. She writes about Marine Corps testimony to the U.S. House Armed Services Tactical Air and Land Forces Subcommittee in which Deputy Commandant for Programs and Resources LtGen Thomas spoke about a new MEF information group that aims to challenge threats in the cyber, electronic warfare, and intelligence realms.

In the third article, we hear an echo of an argument that was previously presented. The Hill authors Phillip Lohaus, Daniel Schuman, and Mandy Smithberger call for each member of the House Intelligence Committee to have a dedicated—and cleared—staff member to help them perform their oversight duties.

As always, I am here to help and answer any questions you may have. Please share your best practices and challenges so that we can continue to learn from each other.

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

Feature Article

The Ten Principles of Intelligence Oversight Program Management

By Mr. John P. Holland
Military Intelligence Professional Bulletin

1. Take assigned responsibilities seriously. While there is a range of additional duties from Safety to Equal Opportunity begging for the attention of the command, only one has two Presidential oversight boards and sub-committees in the U.S. Senate and U.S. House of Representatives, and is unique to Military Intelligence (MI) units–Intelligence Oversight (IO). IO has been the focus of numerous investigations and inquiries from simple command level inquiries to national level with Congressional implications. All questionable intelligence activities (QIA) find their way to the Army Inspector General (IG) who personally reads them all. Needless to say, take it seriously –there is a lot at stake here.

2. Do not appoint the brand new second lieutenant (2LT) as the unit Intelligence Oversight Officer (IOO). It is common practice to groom junior officers by giving them additional duties. It is a great way to teach them the myriad duties necessary to run a unit. It places them in positions to lead, demonstrate initiative, and grow as officers. However, Intelligence Oversight is not one of those developmental opportunities. Army Regulation 381-10 Intelligence Oversight requires commanders to appoint "an experienced MI professional" as the unit IO officer. The problem is that a 2LT is not "experienced." It simply takes years of directing intelligence collection efforts, reading the ensuing intelligence reports to correctly apply the rules under Procedures 2 and 3 and make dissemination determinations under Procedure 4. This is particularly difficult in sensitive open source platforms and in signals intelligence (SIGINT). There is a reason that the National Security Agency requires all employees complete rigorous IO training and possess years of experience before the employee is certified as an IO officer. A new 2LT, not yet familiar with the collection power in an MI unit and how to assess the U.S. Person information it may include, is not the best choice when there are experienced warrant officers and U.S. Government civilians available. Appointing a senior military or a Department of the Army civilian experienced in their craft, preferably across a broad range of intelligence operations, will pay dividends. Additionally, IO is an inherently governmental function that cannot be performed by a contractor.

3. Foster a culture of compliance and oversight. Every MI unit has its own culture. It is a combination of many things: the unit's history, morale, recent deployments, mission, personnel turn-over, and leadership. Some units have a culture reticent to report any QIA or significant/highly sensitive incidents. The rational may be that unit leaders do not want any perceived mistakes on their watch. As a result they often do not report any QIA, or at the very least do not contact higher to discuss collection issues that have a high chance of U.S. Person data being included. This is contrary to intent of DOD 5240-1R Procedures Governing the Activities of DOD Intelligence Components that Affect U.S. Persons. Reporting QIA and significant/highly sensitive matters demonstrates a command's ability to self-regulate and handle the collection authorities it has been given. Fostering a climate of reporting is critical to protecting those mission authorities and can be used as justification for requesting additional collection authorities. Furthermore, IOOs have to often question the risk-to-reward ratio of new intelligence collection platforms. Many new open source intelligence (OSINT) platforms are expensive, redundant, and venture into areas that the public and policy makers have not fully codified their positions regarding the intelligence community's access. This requires someone to ask difficult and unpopular questions at a staff meeting regarding not only the information's value, but how it is to be collected.

4. Automate questionable activity reporting. AR 381-10 (MCO 3800.2B) allows 5 days to report a

QIA. Time is critical in reducing the impact of such incidents. Many units have an automated reporting tool using MS SharePoint on SIPRnet. Some units opt for a reporting tool that is an email alias to key staff members, the IOO and the Staff Judge Advocate (SJA). Regardless of the method, automating the reporting method speeds up the reporting process, increasing accuracy and accountability while providing an auditable process. Most importantly–it shows command involvement.

5. Tailor your training to unit mission and authorities. Simply using a canned set of PowerPoint IO training slides from another unit, briefing them, and checking the proverbial box complete is absolutely the wrong way to conduct IO training. Just like any other training, IO training should be tailored to reflect the unique intelligence processes within the unit or more importantly how the unit actually conducts intelligence collection, processing, maintaining intelligence databases, and the dissemination decision points. Training slides value increases when the unit's intelligence section real names (i.e., the "ACE" or "OSINT Shop") and the names of key positions (i.e., G2 Night Shift "Pit Boss" or ACE Chief) are used. Furthermore, IO training should include examples of potential QIA using examples drawn from the local collection platform capabilities. In short, training customization increases applicability of the lessons and hopefully the likelihood of recognizing a QIA and reporting it.

6. Read and study. No doubt reading a National Security Directive such as PPD-28 Signals Intelligence Activities will induce a near comatose nap. However, to be a true intelligence professional, it is crucial that you read, understand, and apply the rules. Simply put: if you don't read them–you won't know them. Start with AR 10-87 Army Commands, Army Service Component Commands, and Direct Reporting Units [MCO 3800.2B; Oversight of Intelligence Activities & SECNAVINST 5000.34F Oversight of Intelligence Activities, Intelligence Related Activities, Special Access Programs, and Sensitive Activities Within the Department of the Navy], and your unit's authorizing mission documents to determine if you are authorized to collect "raw" intelligence or merely read published intelligence reports. Read EO 12333 U.S. Intelligence Activities, and match its sections with corresponding sections in DOD 5240.1-R and then AR 381-10 [MCO 3800.2B; Oversight of Intelligence Activities]. Doing so will allow you to see the application and intent of each procedure as it has worked its way down from the President, through the Secretary of Defense to the Sectary of the Army. For SIGINT personnel, read EO 13587 Foreign Intelligence Surveillance Act, and applicable U.S. SIGINT directives. For Human Intelligence, the readings should include Defense Intelligence Agency policies. Counterintelligence practitioners should read AR 381-20 [MCO 3850.1J; Policy and Guidance for Counterintelligence (CI) and Human Source Intelligence (HUMINT) Activities] The Army Counterintelligence Program.

7. Ensure access to unit operations orders, intelligence reports, and intelligence databases. Prior to execution, all operations orders should be reviewed by the unit IOO and the SJA. It is far better to prevent a QIA than to go through an investigation later. Too many MI unit IOOs do not routinely check the intelligence reports their units produce or question the dissemination of U.S. Person information their analysts are getting access to and retaining with no thought to the relevance to the unit's foreign intelligence or counterintelligence mission. Again, appointing a seasoned MI warrant officer with full access to the unit databases, intelligence reporting, and all intelligence platforms, to include special access programs can prevent QIAs. Special attention should be paid to open source programs. Remember, conducting the annual files review of unit databases is required by Army Regulation 381-10 [MCO 3800.2B; Oversight of Intelligence Activities]

8. Request the Inspector General inspect your IO program. AR 20-1 [MCO 5430.1; Marine Corps Inspector General Program & MCO 5040; Marine Corps Readiness Inspections and Assessments] Inspector General Activities, requires the command IG inspect intelligence unit's IO program every 2 years. Acting as disinterested third party, the IG can give an MI unit commander an honest assessment of his IO program and will share best practices learned from other MI units. MI unit commanders should

ask to see the previous IG inspection report completed on their unit to determine if the recommendations and finding were implemented. The IG is a valuable asset in running an effective IO program.

9. Map out the intelligence reporting data flow. Data is best visualized like plumbing in a house. Like water, all that intelligence data is going somewhere and is contained in something. Chart the process by which intelligence is collected from the field, processed, analyzed, and the products created and disseminated. Identify where the control measures and internal review processes exist at all levels. Some IOOs have been amazed once they drew the intelligence data flow on a dry-erase board and saw all the intelligence "databases" that grew from a spreadsheet to a system of record. Simply drawing out the intelligence data feeds and following them through the unit's processes, and then out of the unit to customers and labeling the associated authorities at each collection point can be very telling.

10. Leave a legacy. Too frequently what were once very effective IO programs are now dead on arrival. What was the cause of death? The previous IOOs drove the program through the sheer force of rank or personality rather than institutionalizing the procedures of recognizing and following the rules and reporting QIAs. As a result, when they left the unit, the procedures were not modeled and passed on like a battle drill to the next group of Soldiers. Making IO part of the everyday operational considerations is the sure way to leave an endowment at every MI unit. IOOs should emphasize that QIA reporting is not punitive. The root cause may be with the policy that is inconsistent, incorrect, contradictory, or obsolete. The problem may reside in training (not done, incorrect, inconsistent, incomplete, not tailored enough to what Soldiers needed), or it may be communication (poor propagation of policies, incorrect command emphasis, failure to provide left/right limits). The issue may be with an individual who is willful, or negligent. The point is to review what went wrong, why it went wrong, and enact measure to prevent recidivism and foster a climate of continuous improvement.

Mr. Holland has served as the DOD Senior Intelligence Oversight Official since August 2015. His former DA civilian positon was Deputy Intelligence Oversight Advisor to the Commander, U.S. Army Intelligence and Security Command. He is a retired U.S. Army MI officer, having served in various staff and command positions for over 20 years and served in Operations DESERT SHIELD/STORM and with the JCIU, Afghanistan. He is graduate of CAS3, Command and General Staff College, and the Information Resources Management College, National Defense University. He holds graduate degrees from Webster University and Liberty University, and is a 1986 Distinguished Military Graduate of Elon College.

U.S. Marine Corps Looking to Stand Up Information Warfare MEF

By Sandra Jontz
Signal Magazine

With a little more financial backing, the U.S. Marine Corps is primed to grow its force in three critical areas to meet the threats of the future: cyber, electronic warfare (EW) and intelligence.

The nation's expeditionary service is creating what Commandant Gen. Robert Neller, USMC, has called a Marine Expeditionary Force (MEF) information group—a critical component that encompasses those three key warfare domains, Lt. Gen. Gary Thomas, USMC, deputy commandant for Programs and Resources, told members of the U.S. House Armed Services Tactical Air and Land Forces Subcommittee.

"Our perspective is now broadening in terms of additional capabilities that we would need when [troops are] going force-on-force and being able to counter some of the [electronic warfare] capabilities that our adversaries are developing," Gen. Thomas said.

The Corps wants to grow its active duty force by roughly 3,000 Marines, for total end strength of 185,000, he said, with a good amount of growth taking place in those three critical information group areas, he said. "We're also seeing the nexus of cyber and EW, and it's about providing the equipment that allows you to do that, but also now, the organization that gives you that capability as well," he said of the creation of this MEF information group.

Gen. Thomas also addressed the adverse effects that sequestration and years of relying on budgetary continuing resolutions have had on the Marine Corps' ability to modernize its current force and be ready and capable to engage in emerging threats.

Sequestration has seriously hampered the Corps' investment in modernization, which has slumped to a low of 7 percent of its budget. "This is a dangerous trend that we must reverse for the nation's expeditionary force in readiness," he told lawmakers on Friday.

Corps leaders anticipate increasing the investment portion to about 10 percent in fiscal year 2018, with an eventual goal of 15 percent, Gen. Thomas said. The Corps' seemingly disproportionate investments in aviation versus ground equipment concerned Rep. Niki Tsongas (D-MA).

"For many years, the Marine Corps has requested and received vastly more funding for procuring aircraft as compared to ground equipment," she said. "While the Marine Corps certainly has a need for aircraft of many types, the ratio of spending on aircraft compared to ground equipment is striking."

In fiscal year 2016, the Corps appropriated $1.5 billion for ground equipment and ammunition, compared with $5.3 billion for five key aircraft programs: the F-35 Joint Strike Fighter, CH-53K King Stallion helicopter, V-22 Osprey, AH-1 Cobra attack helicopter and KC-130 refueling tanker.

"I would characterize our modernization portfolio as balanced," Gen. Thomas offered. "We're not balanced across the Marine Corps because we haven't been able to put as much into modernization as we'd like, but in terms of the resources we have been able to apply toward modernization, we do feel like we are balanced. We have several needs, both on the aviation side and on the ground side.

"It is true that we have a 3-to-1 ratio in terms of aviation versus ground," he continued, "But a lot of that is just the nature of [the cost of] aviation platforms and the relative expense to ground equipment."

Readiness suffers nearly as much as the Corps' modernization efforts, Gen. Thomas testified, particularly in aviation. "Overall, the readiness of aviation forces and the number of pilot hours per month is still much lower than we would like. The readiness we desire for our aviation is about 75 percent of our fleet," he said, referring to the percent of aircraft that are mission-ready versus those in for routine maintenance.

"Nominally, across the entire fleet, we are down to around 45 percent," he shared to the shock of Rep. Michael Turner (R-OH).

The future operating environment for the Marine Corps is a complex terrain characterized by technology proliferation, information warfare and the need to shield and exploit signatures and operate in an increasingly non-permissive maritime domain, Gen. Thomas said. "As we continue to spend limited resources to sustain legacy systems and develop for threats of the past, we steadily risk losing our competitive advantage against adversaries."

Improving Congress's Oversight of the Intelligence Community

By Phillip Lohaus, Daniel Schuman, and Mandy Smithberger
The Hill

The federal government spent more than $70 billion last year on the Intelligence Community. Are these dollars well spent? Hard to tell. With the pervasive secrecy surrounding its operations, it is

difficult to determine the extent to which the money was spent protecting our national security or invading our privacy.

The reality is that we must look to Congress for the answer—a Congress whose intelligence oversight budget is a pittance, and whose intelligence committees are so disjointed that the 9/11 Commission called for wholesale reform. As the first branch of government, Congress is responsible for legislation and oversight, powers that have been largely relinquished to an over-powerful and under-responsive Executive Branch.

And yet few have full confidence in the ability of the House Intelligence Committee to perform properly. The committee does not have the necessary resources to do its job. Last year the Committee had a 33-person staff and a $3.8 million dollar budget (the Intelligence Community's budget is 18,421 times larger). By comparison, more than 2.8 million people had access to classified information in 2015, including 1.2 million at the top secret level.

So it's not surprising that additional measures are being considered to make up the difference. Members of Congress are calling for a separate, select committee to investigate the claims of Russian hacking of the U.S. election. Many in Congress wish to establish an independent encryption commission. And though the Intelligence Community has had many successes, its failures—such as not foreseeing the Arab Spring, misleading Congress about the scope and nature of the threat of terrorism, and not thwarting foreign interference in U.S. elections—would be fewer if the House Intelligence Committee was better positioned to keep an eye on the myriad programs and employees that populate our national security bureaucracy.

In addition, the intelligence community, whose leadership recently refused to brief its members on the election hacking scandal, does not treat the congressional Committee seriously. Despite the protests of the Committee Chairman Devin Nunes who wrote, "The legislative branch is constitutionally vested with oversight responsibility of executive branch agencies, which are obligated to comply with our requests," the decision was not reversed and the complaints were ignored, seemingly without consequence.

Technological changes have created new threats and opportunities, and the challenge of understanding the craft and actions of our intelligence officials has become increasingly complex. Unfortunately, the widespread perception today is that Congress is no longer willing or able to fulfill its original goal of reforming and overseeing the intelligence bureaucracies.

While much should be done, there is an obvious place to start: *Committee members should have a dedicated staffer—with the necessary clearances—working on intelligence matters.* This simple idea already is in place in the Senate, where individual members of the Senate Intelligence Committee have the benefit of committee staff (whose loyalties are to the committee's leadership) and a personal staffer who works at that member's direction. It would have the additional benefit of significantly expanding the number of House staffers dedicated to overseeing intelligence matters. The current system stymies the agency of individual members of Congress, reduces transparency, and decreases the likelihood that whistleblowers will bring concerns to the attention of key members. Expanding oversight duties to include the perspectives of all committee Members will mitigate these risks.

To their credit, eight members of the House Intelligence Committee have recognized this shortfall, signing a letter in support of dedicated intelligence staffers. The support of a few more members is needed to reach a committee majority, and the rest of the House too must be persuaded. While much more should be done, as was discussed in a recent White Paper sponsored by a variety of stakeholders, this easy first step should be seriously considered.

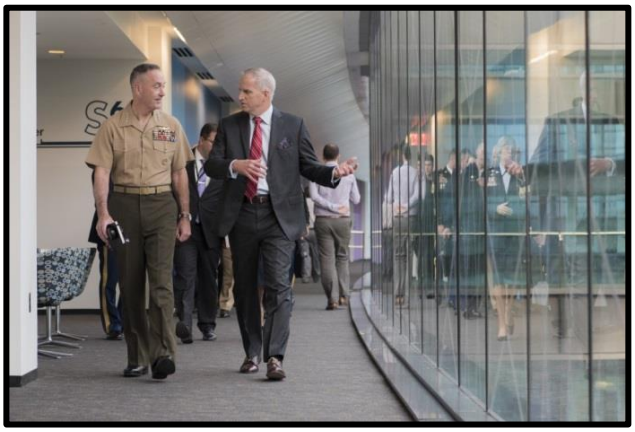
If Congress does not effectively oversee this critical component of national security, they will continue

to play catch-up when the intelligence community falters. Congress provides the public's only view into the most secretive aspects of the national security bureaucracy, and it's time for Americans to empower and enable Congress to fulfill this solemn and irreplaceable duty to oversee it.

Phillip Lohaus is a Research Fellow at the American Enterprise Institute, Mandy Smithberger is Director of the Straus Military Reform Project at the Project on Government Oversight, and Daniel Schuman is Policy Director at Demand Progress

Intelligence Photographs in the News

Marine Corps Air Ground Combat Center Twentynine Palms, CA. - Sgt. Sean McGoldrick, a ground intelligence analyst with 1st Combat Logistics Battalion attached to 1st Marine Regiment, 1st Marine Division, and Cpl. David Adames, an intelligence analyst with 1st Marine Regiment, 1st Marine Division, make adjustments to the RQ-11B Raven UAS during Steel Knight 17. Steel Knight is a division level exercise to enhance the command and control and interoperability with the 1st Marine Division, its adjacent units and naval support forces. **Photo By: Lance Cpl. Austin Mealy**



Springfield, VA - Marine Gen. Joseph F. Dunford Jr., chairman of the Joint Chiefs of Staff, speaks to Robert Cardillo, Director of the National Geospatial-Intelligence Agency, Oct. 24th 2016. The NGA delivers world-class geospatial intelligence that provides a decisive advantage to policymakers, warfighters, intelligence professionals and first responders. **Photo By: Petty Officer 2nd Class Dominique Pineiro**

Durham, North Carolina - Lt. Gen. Vincent R. Stewart speaks to students and staff of North Carolina Central University, University of North Carolina at Chapel Hill, Duke University and North Carolina State University about the opportunities in the U.S. Intelligence Community at in Durham, N.C., March 3, 2017. After the keynote address, Stewart, along with Col. Dimitri Henry, Col. Jerry Carter, and Lt. Col William Wilburn, engaged in a Q&A segment. **Photo By: Sgt. Antonio J. Rubio**

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, DoD Dir 5240.01, DoD Reg 5240.1-R, SECNAVINST 3820.3E, 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 5000.34E

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 5000.34E**

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.