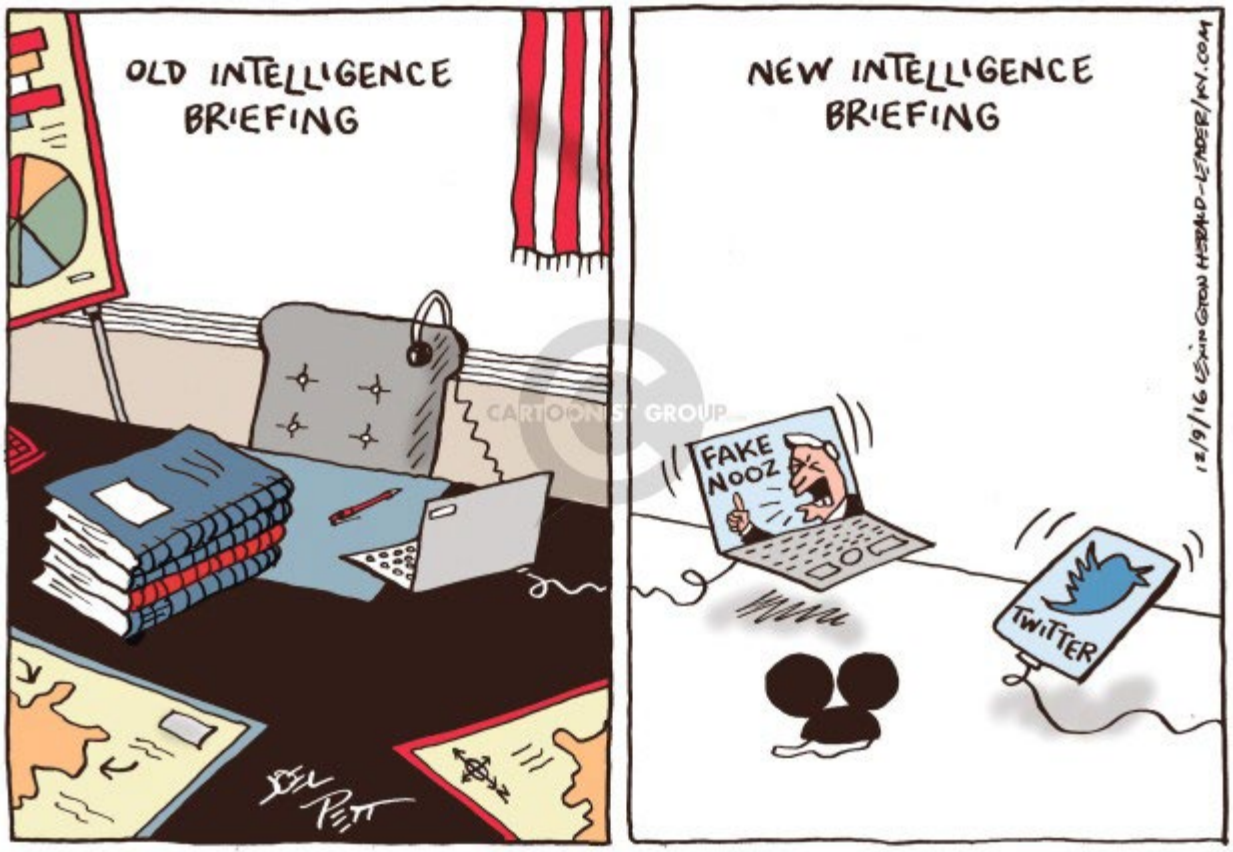
OVERWATCH

"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 15 Issue 2 Winter 2024

IN THIS ISSUE, FEATURED ARTICLE: 2024 PRIORITIES FOR THE INTELLIGENCE COMMUNITY



Inspector General of the Marine Corps

The Inspector General of the Marine Corps (IGMC) facilitates Marine Corps efficiency, integrity, and institutional readiness through objective and independent assistance, assessments, inspections, and investigations to enhance the Marine Corps' mission success and the welfare of its Marines, Sailors, and their families.

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
Deputy Director **VACANT**
LtCol Bessie Bernstein -Sensitive Activities Officer

Inside This Issue

3 A Message from the Director

4. 2024 Priorities for the Intelligence Community

7. House Intelligence Committee Advances FY25 Intelligence Authorization Act

7. Intelligence History

10. Intelligence Photographs in the News

Web Links

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

Marine Corps Inspector General
https://www.hqmc.marines.mil/igmc//

Naval Inspector General
https://www.secnav.navy.mil/ig

Intelligence News
INTEL - Home

A Message from the Director

Greetings from the Office of the Inspector General for the Marine Corps, Intelligence Oversight Division. This edition of *Overwatch* is the second of calendar year 2024. As always, the articles provided in this issue do not represent the opinion of Intelligence Oversight Division or the Office of the Inspector General. The articles are meant to inspire thought and create a space for discussion.

SECNAVINST 3820.F, INTELLIGENCE OVERSIGHT WITHIN THE DEPARTMENT OF THE NAVY is currently in rewrite and will be published shortly. Please keep an eye out for it. MCO 3800.2C is also moving through the process to be updated. The Functional Area Checklist 3800 INTELLIGENCE has been modified and in final stages of review before being published.

The annual training requirement for Intelligence Oversight can be fulfilled by successful completion of the online Annual Intelligence Oversight Training course currently available via Marine Net at: https://portal.marinenet.usmc.mil/content/mnet-portal/en/catalog/coursedetails.html?courseid=cb536883-529f-453d-bbad-3d186063d5d0

The course takes approximately one hour to complete. Completion status will be captured in personnel's Marine Net profile and recorded in the Marine Corps Total Force System (MCTFS) for unit training managers' documentation. Note that course completions remain valid for one year from completion.

I am very pleased at the amount of personnel utilizing this new training format. Numbers of personnel taking the training is rising exponentially.

The first article discusses priorities for the Intelligence Community

Our second article discusses the FY25 Intelligence Authorization Act

Last, we have our section on Intelligence History which this issue continues with excerpts on the Birth and Early Years of Marine Corps Intelligence.

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

2024 Priorities for the Intelligence Community

Congressional Testimony from Ms. Kari Bingen, Former Deputy Under Secretary for Intelligence May 15, 2024

Kari Bingen spoke on a House Permanent Select Committee on Intelligence panel about the acute security challenges facing the United States, the technology trends occurring around us, and the significant changes underway to posture the intelligence community (IC) for the competitive and contested environment we face.

I cannot overemphasize how acute the security challenges are before us, the technology trends occurring around us, and the significant changes underway to posture the intelligence community (IC) for the competitive and contested environment we face. Adversary threats are increasing in speed, scale, and complexity, and are made even more difficult by the increasing collaboration across threat actors and simultaneity of crises and challenges upon us. We will have to question our assumptions, our policies and processes, and our ways of conducting intelligence activities that have been enshrined in our thinking over the last several decades.

Today, for your consideration, I offer observations on five aspects of the intelligence enterprise that are vitally important for the United States' maintaining an advantage in this competitive and contested security environment. I make these observations largely through a defense intelligence lens, knowing that my colleagues on this panel complement my knowledge across other areas of the IC and its missions.

Reclaiming our ISR Advantage

First, our intelligence, surveillance, and reconnaissance (ISR) capabilities are under increasing threat while our adversaries' ISR is rapidly advancing. Many of our ISR systems and operating concepts assume air, space, and spectrum superiority. We built large, exquisite satellite systems and controlled overseas drones from ground stations in the United States using satellite communications (SATCOM) and Global Positioning System (GPS) navigation. However, against a sophisticated adversary with anti-satellite weapons, robust air defenses, and ways to jam SATCOM and GPS, these ISR systems and operating models will be increasingly under strain. Such operational threats are driving investments towards more resilient architectures, including proliferated ISR satellite constellations, and networking solutions that create multiple pathways to deliver intelligence data to users.

Meanwhile, foreign advances in ISR, including ubiquitous sensing and artificial intelligence (AI), will make it more difficult for our military forces and intelligence operatives to maneuver undetected. Surveillance cities, sophisticated digital monitoring, and advanced analytic tools employed by our adversaries will make other aspects of intelligence, such as human intelligence (HUMINT) operations and the use of cover, increasingly harder. Such constant surveillance – whether through space, terrestrially, or in cyberspace – will necessitate new or modified capabilities, tactics, training, and tradecraft.

In space, the majority of recently launched Chinese satellites have been ISR satellites, which extend Beijing's surveillance into space. According to U.S. Space Command, as of January 2024, China had approximately 360 ISR satellites on orbit, more than triple the number in 2018.[1] In August 2023, Beijing launched the world's first geosynchronous orbit (GEO)-based synthetic aperture radar (SAR) satellite and in December 2023, it launched an optical imagery satellite to GEO, Yaogan-41. When paired with data from other Chinese ISR satellites, AI to rapidly identify objects, and networked communications systems, the People's Liberation Army (PLA) is quickly closing its own sensor-to-shooter kill chains across the Indo-Pacific.[2] Our military forces will need to train under the assumption that they will be seen, located, and targeted.

Revitalizing Foundational Military Intelligence and Scientific and Technical Intelligence

Second, our peer adversaries are developing more technically advanced and complex military systems that we need to understand to defeat. This will place increasing demands on our foundational military intelligence (FMI) and scientific and technical intelligence (S&TI) capabilities, which received less emphasis over the last 20 years. During this time, China and Russia made substantial progress in developing and fielding hypersonic missiles, anti-

satellite weapons, electronic warfare and cyber-attack weapons, and undersea systems, to name a few.

FMI involves developing a comprehensive understanding of foreign militaries, including their facilities, organizational units, and capabilities. S&TI involves the in-depth technical analysis of foreign weapon systems, including performance, vulnerabilities, how they're networked and controlled, and how they're integrated into broader military operations. This analytic knowledge informs our development of defenses and countermeasures, as well as ways to defeat these systems. S&TI centers, such as the National Space Intelligence Center (NSIC), National Ground Intelligence Center (NGIC), and the Office of Naval Intelligence (ONI), provide such detailed analysis of foreign weapons, air, space, and undersea systems.

I would also call your attention to the Defense Intelligence Agency's (DIA) Machine-assisted Analytic Rapid-repository System (MARS) program – an effort to modernize our master data repository of FMI information. This is critical as today's platform rests on 1980s database technology and is severely limited in capturing richer data sources, more dynamic targets, and newer military activities, including in space and cyberspace, necessary to support intelligence analyses, military operations, and activities with allies and partners.

Harnessing Technological Change from Outside Government

Third, while the IC maintains exquisite intelligence capabilities and proficiencies, I would observe that many of the most consequential technological advancements are occurring in the private sector and are being fueled by private capital. These advancements have the potential to revolutionize how the IC collects and analyzes information, but they will challenge culture and existing ways of doing business.

Generative AI and advanced compute are prime examples of this. Based on research by Goldman Sachs, global AI investments are estimated to approach $200 billion by 2025,[5] in contrast to U.S. government investment at less than $5 billion. The IC cannot replicate private sector AI and compute in scale, speed, or investment. For the IC to take full advantage of large-scale compute and generative AI – wherein machines can contextually learn, synthesize, and generate data across images, signals, and text – it will need to figure out how to work across both large-scale unclassified and classified compute environments.

While at the Pentagon, I recall pressing my daily intelligence briefer to provide deeper insights and context on topics than what I could access via open source. The advances described above can aid analysts in identifying patterns, drawing out unique connections across classified and unclassified datasets, and making sense of vast amounts of data that humans can't process at scale. But we will also need to think through how to harmonize analytic tradecraft and human expertise with machine-generated analysis.

This technology can be harnessed for good but can also lead us astray. Generative AI can create new kinds of deception, obfuscation, and disinformation at machine speeds. The IC must have an in-depth understanding of these technologies in order to develop ways to mitigate such threats. We will need to expand traditional analytic disciplines like foreign denial and deception to account for these technology trends.

There is also a growing tension between the speed and depth of analysis: getting tactical ISR data directly and quickly to warfighters versus providing analysis, context, and verification of information. While this should not be an either-or choice, technological advancements in automation and AI are making possible different constructs for user access to data and information. Particularly in the space arena, private companies operating satellite constellations in the hundreds to thousands are leveraging automation, advanced processing, and AI to optimize their operations and quickly draw insights from collected data. These advancements present opportunities for the IC to think differently about its satellite tasking and dissemination models, allowing for more direct tasking by users, direct downlink of satellite data to tactical nodes, and greater AI-enabled analysis.

A common theme here is that much of these technological advancements are occurring in the private sector, outside of the U.S. Government and outside the United States. We are in a technology race with China, which is after the same advanced technology that we are – AI, aerospace, quantum, microelectronics, biotechnology, etc. – for both military and economic benefit.[7] Many of the trends and insights about this techno-economic competition

will not be found in highly classified reporting, but rather in understanding the flow of private capital, global supply chains, academic research, and business dynamics. Much of this can be gained through greater interaction with the private sector that competes with Chinese entities globally and on a daily basis. There is a need for intelligence analysts to understand this aspect of the global landscape and how U.S. competitiveness affects national security.

Securing our People, Information, and Business Advantage

Fourth, please continue to pay close attention to the security and counterintelligence mission of the IC, including industrial security and personnel vetting. While not a high-profile IC mission or program, security and counterintelligence underpin all activities that the IC and DoD undertake. You know this well, but it bears emphasis: Beijing continues to comprehensively target U.S. technologies, intellectual property, supply chains, and critical infrastructure across government, industry, and academia. It is playing the long game to penetrate our technology base and steal our information, using both legal and illegal means, such as foreign capital, economic espionage, cyber data exfiltration, and talent recruitment programs.

Much of the contact layer being targeted by our adversaries is outside government, in the private sector and academia. This necessitates the importance of education and engagement, as well as greater transparency on foreign threats and tactics, and communicating these in ways that resonate with and move at the speed of business. The National Counterintelligence and Security Center (NCSC) and Defense Counterintelligence and Security Agency (DCSA) are progressing in the right direction: from "checklist-based" approaches to industrial security towards more threat informed, risk-based approaches to assess and mitigate vulnerabilities.

I would also encourage strong oversight of the government's efforts to reform personnel vetting, including improving the clearance review and adjudication process. Continuous evaluation is an important step forward, but continue to push on personnel vetting reforms, reciprocity, and IT system modernization. With access to myriad data sources and advances in data analytics, there are smarter ways to assess and monitor personnel risks than current methods. The IC will simply not be competitive in attracting top, diverse talent if candidates are waiting months or years for a security clearance.

Developing our Workforce

Finally, I would recommend a comprehensive examination of workforce development within the IC. Candidly, this is an area in which I wish I had paid more attention. A big idea for the Committee's consideration is whether personnel reforms analogous to those in the Goldwater Nichols Act of 1986 are needed to guide how the IC manages the career paths and professional development of its workforce. Goldwater-Nichols was a catalyst for enhancing operational effectiveness, building a joint force, and developing more well-rounded military leaders through professional military education and joint assignments that broaden their perspectives and cross service relationships.

While the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 sought some changes similar to Goldwater-Nichols, it did not go far enough and implementation has been mixed. My observation is that the IC could be stronger in how it cultivates its workforce, especially for those seeking promotions into leadership roles. Such career enhancing and stimulating experiences are also important to nurture and retain talent, build collaborative relationships across the IC, and enhance mission effectiveness.

In full disclosure in my role as a member of the National Intelligence University's Board of Visitors, I see greater opportunity for professional education, akin to joint professional military education (JPME). I also see a need to broaden the knowledge and experience base for intelligence professionals – whether in conducting strategic research and analysis outside their day-to-day workflows, understanding their portfolio from different organizational perspectives, or experiencing firsthand the technology, capital, and global competitive dynamics at play through a public-private sector talent exchange. While largely anecdotal, I observed numerous joint duty assignment (JDA) professionals return to home organizations only to be relegated back to similar positions that they had left.

Conclusion

Throughout the Cold War, the United States competed politically and militarily, but never economically, with the Soviet Union. For the first

time, our nation faces a strategic competitor with the resources and potential to match, if not one day exceed, the size and scope of U.S. economic might and to develop new technologies that rival our own. Over the last 40 years, the United States has had to adapt several times to a new geopolitical and strategic environment, first after the collapse of the Soviet Union and then, after the September 11 attacks.

Now 20 years after the IRTPA and the establishment of the Director of National Intelligence, we face yet another new and evolving global landscape. We are still learning how to adapt our intelligence and defense mindsets, processes, and systems to this new environment in which we face an adversary with economic and military potential unlike anything we've faced in the past.
We have a window to get this right and are fully capable of rising to the challenge.

House Intelligence Committee Advances FY25 Intelligence Authorization Act

Washington, D.C., June 12, 2024

The House Permanent Select Committee on Intelligence passed the Intelligence Authorization Act (IAA) for Fiscal Year 2025, which authorizes funding for the United States Intelligence Community (IC). The measure was passed unanimously by voice.

"As America's adversaries become more emboldened, it is imperative that Congress strengthen U.S. national security and make certain that the men and women who serve our country in the Intelligence Community have the tools and resources they need," **said Chairman Mike Turner and Ranking Member Jim Himes.** *"Beijing and Moscow continue to expand their nuclear programs and space-based weapons systems. With authoritarian regimes exploring novel capabilities, the IC must be equipped to perform in all operational environments. The Intelligence Authorization Act for Fiscal Year 2025 takes critical steps to bolster the United States' counterintelligence posture while also calling for greater transparency within the IC and expanding whistleblower protections for past and present IC employees. By passing the FY25 IAA in a bipartisan fashion, the House Intelligence Committee has once again demonstrated its commitment to safeguarding our national security."*

The legislation advances significant bipartisan Committee priorities, including:

Investing in Space Infrastructure

The bill counters Russia and Chinese destabilizing influences by investing in the critical national security space industrial base. It invests in strategic U.S. supply chain sectors and grows strong space acquisition expertise by working with the Space Force acquisition professionals as part of the longstanding military commitment to the National Reconnaissance Office.

Continuing to Address CIA's Response to Sexual Assault and Harassment in the Workforce

The Committee continues to monitor the implementation of the FY24 IAA provision addressing the handling of sexual assault reports inside the CIA. Specifically, the bill modifies the special victim investigator position to ensure investigative objectivity.

Supporting Congressional Oversight to Ensure an Effective CIA

The IAA directs the Government Accountability Office to conduct a study on the CIA's reorganization known as "modernization" to assess its impacts on operational and analytic culture within the agency. This will help ensure the IC adapts to the evolving global security environment.

Taking Next Steps Related to Anomalous Health Incidents (AHIs)

While the Committee's investigation into AHIs continues, the bill authorizes the establishment of an independent commission on the national security and defense risks associated with AHIs

Bolstering Cybersecurity and Counterintelligence Threat Warning

The U.S. continues to see foreign threats on American soil and through nation-state cyber intrusions. This year, the Committee has taken steps to strengthen resilience against foreign counterintelligence and cyber threats. The Committee authorizes

counterintelligence capabilities for the U.S. Coast Guard and increases counterintelligence support for the Department of Energy, provides enhanced oversight at the Department of Treasury and the Department of State, and directs a new awareness program at the FBI to provide information to prevent and mitigate cyber-attacks against critical infrastructure.

Retaining and Recruiting a Strong IC Workforce

The Committee remains dedicated to ensuring the IC recruits and retains top talent. This year, the IAA enhances recruiting efforts for transitioning military servicemembers, placing emphasis on joint duty assignments to cultivate a joint workforce that will improve talent retention, offer career enhancing experiences, and foster collaboration across the IC.

Protecting IC Whistleblowers

The Committee is focused on ensuring IC employees can communicate their concerns to the congressional intelligence committees through the Inspectors General. This year the Committee has included a number of provisions to improve the whistleblower process, including enabling former IC employees to make better use of the "urgent concern" process.

Improving SCIF and Clearance Reform

This year's IAA continues the Committee's focus on enhancing the transparency and structure of the IC. Mirroring the National Defense Authorization Act, this Act directs the sensitive compartmented information facility (SCIF) accreditation mission be assigned to the Defense Counterintelligence and Security Agency (DCSA) for much of the Department of Defense. Further, greater transparency of both personnel security and polygraph timeliness are mandated by the Committee.

Improving Military Counterintelligence

The bill gives special agents with Army Counterintelligence Command the tools they need to fully pursue counterintelligence investigations.

Intelligence In History

The below is the continuation of a series of articles on the history of military intelligence.

Post–World War I Reorganization of the Marine Corps

By Michael H. Decker and William MacKenzie

Until a few years before World War I, the Marine Corps had essentially no Headquarters Staff as we think of today. The Major General Commandant oversaw the Marine Corps through a small personal staff and three staff departments: Adjutant and Inspector, Quartermaster, and Paymaster. It was not until April 1911 that the Office of Assistant to the Commandant was created, headed by Colonel Eli K. Cole, who served as what today would be called a chief of staff. Colonel Cole was replaced in January 1915 by Colonel John A. Lejeune.

Since World War I began in August 1914, the Major General Commandant, as well as the secretary of the Navy and the chief of naval operations, had pushed for increases of manpower and materiel, to include larger staffs. This led to the Naval Act of 1916, which increased the Corps' size by about 50 percent, from 344 officers and 9,921 enlisted to 597 officers and 14,981 enlisted.4 It also authorized emergency increases up to 693 officers and 17,400 enlisted, which occurred on 26 March 1917. The act allowed for 8 percent of the officers, or 55 of the 693, to serve in the staff departments.

By fall 1918—after Marines had fought in Belleau Wood, Soissons-Château-Thierry, and Saint-Mihael—the 12th Major General Commandant, George C. Barnett, decided to create a planning section. On 19 December 1918, the Headquarters Planning Section was established and charged with "all matters pertaining to plans for operations and training, intelligence, ordnance, ordnance supplies and equipment." At first, the Planning Section, under direct supervision of the Office of the Assistant to the Commandant, only had three officers.

World War I was a driving factor in the decision to create a Planning Section, with intelligence as one of many functions identified for improvement based on shortcomings experienced during the war. During World War I, Marine officers interacted with and

learned from other branches of the AEF and other armies, such as the French. The Army's Military Intelligence Division (MID) and the U.S. Office of Naval Intelligence (ONI) were larger and more sophisticated than the Marine Corps' intelligence efforts and staff organization. It is likely that the Marine Corps staff developed its own small intelligence section after World War I based on experience with the larger ONI and MID organizations.

Major General Lejeune became the Major General Commandant on 1 July 1920 and brought his experience of commanding the 2d Division in the AEF and extensive use of a European staff system in those organizations to Headquarters. On 1 December 1920, Lejeune reorganized Headquarters and created the Division of Operations and Training, with Brigadier General Logan Feland as its first director. The Division of Operations and Training included Operations, Training, Materiel, Aviation, and Military Intelligence sections. Creation of the Military Intelligence Section represents the first permanent Marine Corps intelligence organization. Brigadier General Feland assigned Lieutenant Colonel Earl H. Ellis, who had been his brigade intelligence officer in the Dominican Republic, as the first head of the Military Intelligence Section.

Next up- Military Intelligence Section Activities

FORT BONIFACIO, PHILIPPINES
05.24.2024
Photo by Staff Sgt. Dana Beesley
13th Marine Expeditionary Unit

Service members of the Philippine Navy, Philippine Marine Corps, Philippine Air Force, and U.S. Marine Corps pose for a group photo during an intelligence analyst to analyst subject matter expert exchange at Fort Bonifacio, Manila, Philippines, during Archipelagic Coastal Defense Continuum May 24, 2024. ACDC is a series of bilateral exchanges and training opportunities between U.S. Marines and Philippine Marines aimed at bolstering the Philippine Marine Corps' Coastal Defense strategy while supporting the modernization efforts of the Armed Forces of the Philippines. (U.S. Marine Corps photo by Staff Sgt. Dana Beesley)

U.S. Marine Corps Lance Cpl. Derick Cordova, a native of Connecticut and an infantryman with 3rd Littoral Combat Team, 3rd Marine Littoral Regiment, 3rd Marine Division, sights in on a Multi-Purpose Anti-Armor Anti-Personnel Weapons System while participating in an Advanced Infantry Marine Course during the Archipelagic Coastal Defense Continuum at Paredes Air Station, Philippines, May 29, 2024. This training was conducted alongside Philippine Marines with Marine Battalion Landing Team 10. ACDC is a series of bilateral exchanges and training opportunities between U.S. Marines and Philippine Marines aimed at bolstering the Philippine Marine Corps' Coastal Defense strategy while supporting the modernization efforts of the Armed Forces of the Philippines. (U.S. Marine Corps photo by Cpl. Malia Sparks)

U.S. Marine Corps Capt. Daniel Donlon, an intelligence officer with 13th Marine Expeditionary Unit, conducts a guided discussion on analyzing topographical maps as part of an intelligence analyst to analyst subject matter expert exchange at Fort Bonifacio, Manila, Philippines, during Archipelagic Coastal Defense Continuum May 24, 2024. ACDC is a series of bilateral exchanges and training opportunities between U.S. Marines and Philippine Marines aimed at bolstering the Philippine Marine Corps' Coastal Defense strategy while supporting the modernization efforts of the Armed Forces of the Philippines. Donlon is a native of Illinois. (U.S. Marine Corps photo by Staff Sgt. Dana Beesley)

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):** Intelligence Oversight ensures that all activities performed by intelligence units and personnel are conducted in accordance with federal law, Presidential Executive Orders, DoD directives, regulations, policies, standards of conduct, and propriety References: E.O. 12333, DoDM 5240.01, DoD Reg 5240.1-R, SECNAVINST 3820.3F,SECNAVINST 5000.34G, MCO 3800.2B

ii. **INTELLIGENCE RELATED ACTIVITY**. Activities that are not conducted under the authority of Executive Order 12333 that involve the collection, retention, or analysis of information, and the activities' primary purpose is to: a. train intelligence personnel; or b. conduct research, development, or testing and evaluation for the purpose of developing intelligence-specific capabilities. Reference: SECNAVINST 5000.34G.

iii. **SENSITIVE ACTIVITIES:** Operations, actions, activities, or programs that are generally handled through special access, compartmented, or other sensitive control mechanisms because of the nature of the target, the area of the operation, or other designated aspects. Sensitive activities also include operations, actions, activities, or programs conducted or supported by any DoD component, including the DON, that, if compromised, could have enduring adverse effects on U.S. foreign policy, DoD or DON activities, or military operations; or cause significant embarrassment to the United States, its allies, the DoD, or DON. Reference: SECNAVINST 5000.34G.

iv. **SPECIAL ACCESS PROGRAM (SAP):** A program activity that has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within the SAP is identified by a security classification guide. DoD SAPs are divided into three categories: Acquisition SAP; Intelligence SAP; or Operations and Support SAP. Reference: SECNAVINST 5000.34G.

v. **QUESTIONABLE INTELLIGENCE ACTIVITY:** Any intelligence or intelligence-related activity, when there is reason to believe such activity may be unlawful or contrary to any Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity. Reference: SECNAVINST 5000.34G.

vi. **SIGNIFICANT OR HIGHLY SENSITIVE MATTER (S/HSM)**: An intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an E.O., Presidential directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential Congressional inquiries or investigations, Adverse media coverage, Impact on foreign relations or foreign partners, Systemic compromise, loss, or unauthorized disclosure of protected information.