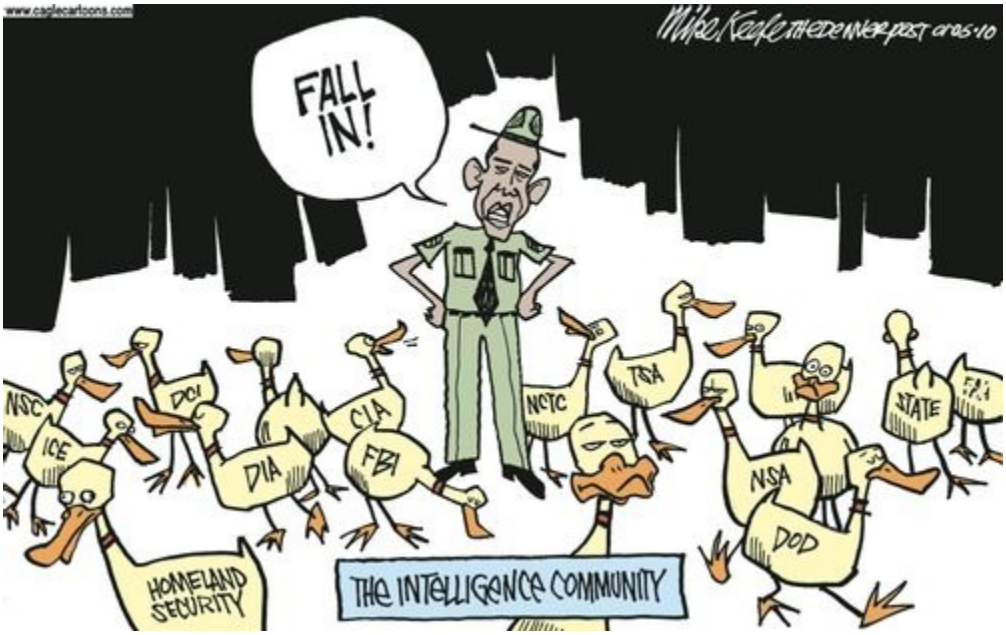
OVERWATCH

"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 1 Winter 2024

IN THIS ISSUE, FEATURED ARTICLE: CONGRESS MUST STRENGTHEN OVERSIGHT ON INTELLIGENCE SHARING AND CIVILIAN HARM



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.

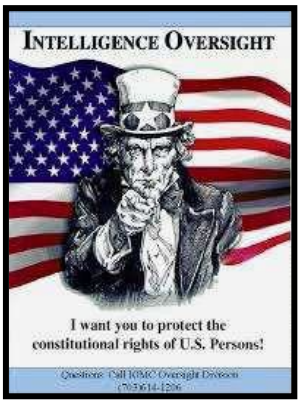
Contact Information Mail:

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
LtCol Kira Parrish, Deputy Director
LtCol Bessie Bernstein -Sensitive Activities Officer

Inside This Issue



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 first 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.

In accordance with DoD Directive 5148.13, and as per MCO 3800.2(C)) soon to be published, all Marines, civilian and contractor personnel assigned or attached to an intelligence unit are required to take annual Intelligence Oversight training. This directive also applies to personnel performing intelligence work as additional duty, even if they are not assigned to an intelligence unit or billet.

This annual training requirement can now 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 strengthening oversight on intelligence sharing and civilian harm.

Our second article reports on Congress pitting privacy against the use of surveillance tools.

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

Congress Must Strengthen Oversight on Intelligence Sharing and Civilian Harm
by Steven Katz and John Ramming Chappell

January 25, 2024

The House Permanent Select Committee on Intelligence (HPSCI) sent an important bipartisan signal through Section 439 of the FY 24 Intelligence Authorization Act (IAA) that the U.S. Intelligence Community (IC) must do more to track how intelligence-sharing with allies and partners may contribute to civilian harm. While the Department of Defense (DOD) is required to report to Congress when a U.S. military operation kills civilians, intelligence agencies – until now – have not been required by law to track or report instances when the United States provides intelligence support for operations that result in civilian harm. Section 439 imposes a requirement to do just that.

Tracking and investigating how partners and allies use U.S. intelligence is important not only because of U.S. legal (and moral) culpability in the strikes it enables, but also to hold partners accountable and instill better civilian protection measures. As the United States continues to work more with partner forces, including through proxy warfare programs such as 127e and 1202, it will be even more crucial for Congress to keep tabs on how partners use U.S intelligence information.

Examining the Intel Sharing Problem

Section 439 of the IAA, which was enacted last year as Section 7326 of the National Defense Authorization Act (NDAA) for Fiscal Year 2024, requires the Office of the Director of National Intelligence (ODNI) to submit an annual report to Congress on civilian casualties caused by foreign government operations, including operations in which intelligence shared by the IC played a "significant role." The provision requires ODNI report the following information: the date on which, and the location where, the operation occurred; the element of the foreign government that conducted the operation; the individual or entity against which the covered operation was directed; and other circumstances or facts that the Director of National Intelligence determines relevant.
Due to the lack of a statutory requirement until now, it is unlikely that either the IC or Congress have a full picture of where shared U.S. intelligence has led to civilian harm. But public reporting has brought to light concerning incidents where U.S. partners likely used U.S. intelligence in military operations that harmed civilians.

For example, members of Congress were alarmed by reports that the United States provided the Nigerian armed forces with intelligence related to a strike of an internally displaced persons camp in Rann, Nigeria that killed over 70 people and wounded at least 120.

Public reporting also indicates that the U.S. military has shared intelligence with Saudi and Emirati forces, enabling their bombing campaign in Yemen that has been widely criticized for indiscriminate attacks.

Absent stronger oversight, it is impossible to discern how allies and partners are using U.S. intelligence in military operations. In certain cases, the IC may be providing indirect support through intelligence sharing for partner operations conducted in a manner inconsistent with U.S. law and policy (including standards set, for example, in the DoD Law of War Manual and the Presidential Policy Memorandum on direct action).

The State Department has developed guidance to investigate reports of civilian harm involving weapons from the United States and recommend actions that could include suspension of arms sales. The same should be required for the sharing and use of U.S. intelligence information.

What Next?
The HPSCI provision is a positive first step that will increase congressional oversight and executive branch transparency of intelligence sharing. But opportunities exist to strengthen the provision further, as Congress has done for the annual 1057 civilian casualty report. Ultimately, the IC and DoD's interpretation and implementation of the statute will determine the annual report's efficacy.

First, the ODNI will need to develop a definition to determine whether intelligence shared meets the "significant role" threshold for inclusion in the annual

report to Congress. Will ODNI's reports only include incidents where the U.S. provided tactical, real-time intelligence for targeting purposes? Or will reporting encompass intelligence provided prior to the strike to initially identify the person or object as a target? A broad definition would help Congress surmise the true scale of the issue and assess the impact of U.S. contributions.

Second, the IAA provision also specifies that covered operations include those conducted by a "foreign government." But the United States may also provide intelligence to non-state entities, including state-supported militias and proxy groups. Congress should modify the provision to ensure "covered operations" include all foreign entities, including non-state actors, using U.S. intelligence for military operations.

Additionally, the provision does not cover all instances of U.S. intelligence sharing that may result in civilian harm. The IAA provision mandates reporting by ODNI, but other entities outside of the IC, such as the combatant commands (e.g., CENTCOM and AFRICOM) also share intelligence with partners. These entities are even more likely to share the type of tactical intelligence that results in civilian harm. The provision should be amended to include all agencies and components that share intelligence with foreign partners, regardless of their status as a member of the IC.

Finally, increased transparency concerning the scale and impact of U.S. intelligence sharing is crucial to support legislative deliberation and public discourse. The IAA provision focuses on providing classified information to Congress; a redacted and declassified version of the report also should be released to the public.

U.S. intelligence is a national asset and should only be used in ways consistent with U.S. law and policies. If partners and allies are not living up to these standards, then Congress must act to do something about it.

Congress pits privacy against intelligence as it ponders surveillance renewal

FBI searched through collected data for information on U.S. persons nearly 5 million times over three years, board reports

Privacy hawks and intelligence-focused lawmakers are expected to battle this year over the reauthorization of a powerful but controversial spy authority, with members at odds over privacy protections and no clear sign where Congress will land.

Lawmakers face an April 19 deadline to reauthorize Section 702 of the Foreign Intelligence Surveillance Act before it expires. But they disagree on how far Congress should go in providing privacy protections on American information that's swept up under the program — and seem to have put the issue on the back burner for now.

Congress failed to pass a longer-term reauthorization in the final days of last year's legislative calendar, with House Republicans clashing over proposals from the Judiciary and Intelligence committees. Instead, faced with the prospect of the authority expiring at the end of last year, lawmakers opted to use the fiscal 2024 defense policy bill to pass a short-term reauthorization through April 19, giving themselves more time to work on a longer-term reauthorization.

Section 702 allows the U.S. government to collect digital communications of foreigners located outside the country. But the program has been the subject of lawmaker concern because it also brings in the communications of Americans and allows the FBI to search through the information without a warrant. The agency can search through the data based on a single field, such as an email address or name.

The debate over Section 702 has cooled since lawmakers returned in the new year and the short-term measure in place, even with members still at odds over what changes are needed.

A bipartisan bill backed by members of the Judiciary Committee would put in place a robust warrant requirement regarding information on Americans, with certain exceptions. The Biden administration has opposed the idea of a warrant requirement.

Another bipartisan bill backed by the Intelligence Committee would prohibit, with exceptions, the FBI from conducting searches of Section 702 for information solely designed to find evidence of criminal activity.

Senate Judiciary Chair Richard J. Durbin, D-Ill., said he does not think there are ongoing negotiations on Section 702 and that lawmakers are "preoccupied with other issues." "But we know we have to get back to it," Durbin said. Rep. Jerrold Nadler, the top Democrat on House Judiciary, said attention in Congress is elsewhere as of right now.

"Everybody's focused on the budget, immigration, Ukraine. Our plate is full now," Nadler said. Rep. Andy Biggs, R-Ariz., who introduced the House Judiciary bill, said he is trying to get Speaker Mike Johnson, R-La., to put the Judiciary panel bill on the floor.

Rep. Pramila Jayapal, D-Wash., another supporter of the House Judiciary bill, said she has not heard about any negotiations regarding Section 702 as of late.

"I've spoken to Andy Biggs quite a bit about this. And we're trying to figure out how to ramp up the momentum again and the pressure," Jayapal said. Jayapal noted that the Judiciary bill passed overwhelmingly in committee. "We think that should be brought up to the floor. But obviously with the extension, we're worried that the momentum that we had built has kind of slipped," she said.

FBI 'misuses'

Justice Department and intelligence officials faced a skeptical Congress after revelations detailed FBI misuses of Section 702 and the broader Foreign Intelligence Surveillance Act. In one revelation, a court opinion said the FBI improperly searched foreign surveillance information using the last names of a U.S. senator and a state-level politician.

Concerned lawmakers have also zeroed in on the apparent scope of the FBI's use of the program. The Privacy and Civil Liberties Oversight Board, which is an independent U.S. government board, reported that the FBI alone searched Section 702 databases for information on U.S. persons nearly 5 million times over three years. A board report said Section 702 "remains highly valuable to protect national security, and that it creates serious privacy and civil liberties risks."

Intelligence-focused lawmakers have acknowledged the misuse of Section 702 and said changes are needed, but the lawmakers have also defended FISA and described the authority as a critical tool in protecting national security.

"We are currently at the highest threat to national security to the United States in a decade. FISA is our best weapon to combat the threats we face today and in the future," said Intelligence Committee Chairman Michael R. Turner, R-Ohio, at a December meeting. "The American people are looking for us to keep them safe."

Turner commented that the FBI has abused Section 702 and said the legislation from his committee includes "targeted reforms." Biden administration officials have underscored the effectiveness of the surveillance authority in making their pitch to Congress, reporting that the program has identified foreign ransomware attacks on U.S. infrastructure and disrupted planned terrorist attacks.

A watered-down surveillance program could leave the agency paralyzed to respond to threats, FBI Director Christopher Wray warned lawmakers in December. Wray also invoked the Sept. 11 terrorist attacks as he delivered a full-throated defense of the program.

"What could anybody possibly say to victims' families if there was another attack that we could have prevented if we hadn't given away the ability to effectively use a tool," Wray told lawmakers on the Senate Judiciary Committee.

As efforts to change the FISA process have stalled, so too have court challenges to the existing law. Earlier this month, the Supreme Court declined to hear an appeal from X, the social media company formerly known as Twitter, that sought to disclose in aggregate requests the company received under both the FISA process and a separate National Security Letter process.

The lawsuit, which has gone on for nearly a decade, came after the FBI blocked the social media site's effort to publish a "Transparency Report" in 2014 containing information about the national security requests it had received. A framework similar to the one the FBI used to block the publication was adopted in the 2015 reauthorization of the FISA law and

allows some disclosures of information about national security requests companies received.

The social media site challenged the FBI decision, arguing it violated the company's free speech rights. But the district court and eventually U.S. Court of Appeals for the 9th Circuit both backed the FBI — decisions the Supreme Court left in place earlier this month.

Several free speech groups weighed in on the case and criticized the Supreme Court's decision not to take the dispute. Patrick Toomey, director of the ACLU's National Security Project, criticized the "sweeping gag orders" upheld by the 9th Circuit decision.
"The government often turns to companies to assist with surveillance, forcing platforms like X to turn over sensitive information about their users while gagging them from providing important transparency to the public," Toomey said.

The First Amendment Clinic at Arizona State University filed a brief to urge the justices to take the case, arguing that the 9th Circuit ruling ignored important free speech interests in denying Twitter's effort to publish its transparency report.

Gregg Leslie, a law professor at ASU and director of the clinic, said that while prior reauthorization efforts have emphasized some transparency, such as the 2015 one that included the current limited disclosure provisions, he has not seen as much momentum for transparency this time around.

Intelligence In History

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

The Birth and Early Years of Marine Corps Intelligence.

By Michael H. Decker and William MacKenzie

To institutionalize the intelligence experiences gained by the American Expeditionary Forces (AEF) in World War I, the U.S. Army published its first doctrinal publication on Intelligence in 1920, *Intelligence Regulations*. On 18 August 1921, the Major General Commandant of the U.S. Marine Corps sent three copies of this classified Army publication to the commanding general at Marine Barracks, Quantico, Virginia. The letter was signed by Brigadier General Logan Feland "by direction" and the receipt was returned signed by a future Commandant, Lieutenant Colonel Thomas Holcomb, then chief of staff to Brigadier General Smedley D. Butler.

To understand what might cause this high-level transfer of an Army doctrinal publication, it is instructive to look at what was going on across the Marine Corps at this time. In the early years after World War I, veterans of the AEF worked to apply lessons learned on staff and unit organization, combined arms, and other tactics, techniques, and procedures to the organization of the Marine Corps for warfighting and at Headquarters Marine Corps.

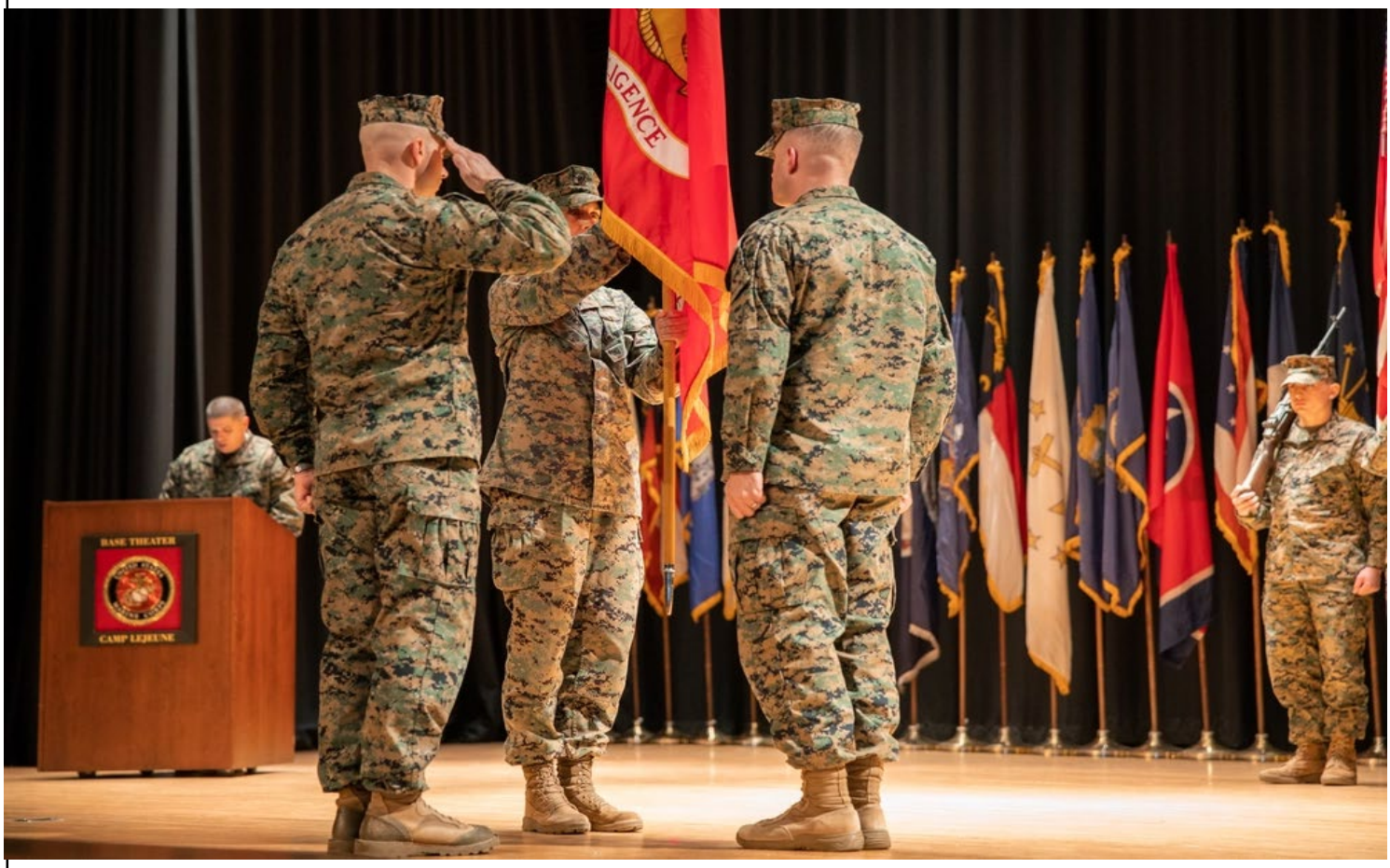
This was especially true of intelligence. Intelligence Marines often point to the 1939 re-organization of Headquarters Marine Corps and cite the creation that year of the staff M-2 as the birth of Marine Corps Intelligence. Marines are not alone in the view that World War II or the run-up to it began the formal approach to the craft of intelligence.

Many in the national intelligence community point to the creation of the Office of Strategic Services as the birth of the intelligence community; prior to that, there was no dedicated or formal U.S. intelligence service outside of the military. As former intelligence officer Dr. Mark Stout asserts, "Historians and practitioners generally date the origins of modern American intelligence to the Office of Strategic Services (1942–1945) and the National Security Act of 1947 which created the CIA and the U.S. Intelligence Community."

However, an analysis of how the intelligence lessons learned from World War I resulted in organizational changes in the interwar years reveals significant intelligence activity in the Marine Corps during that period and predates the 1939 reorganization of Headquarters Marine Corps.

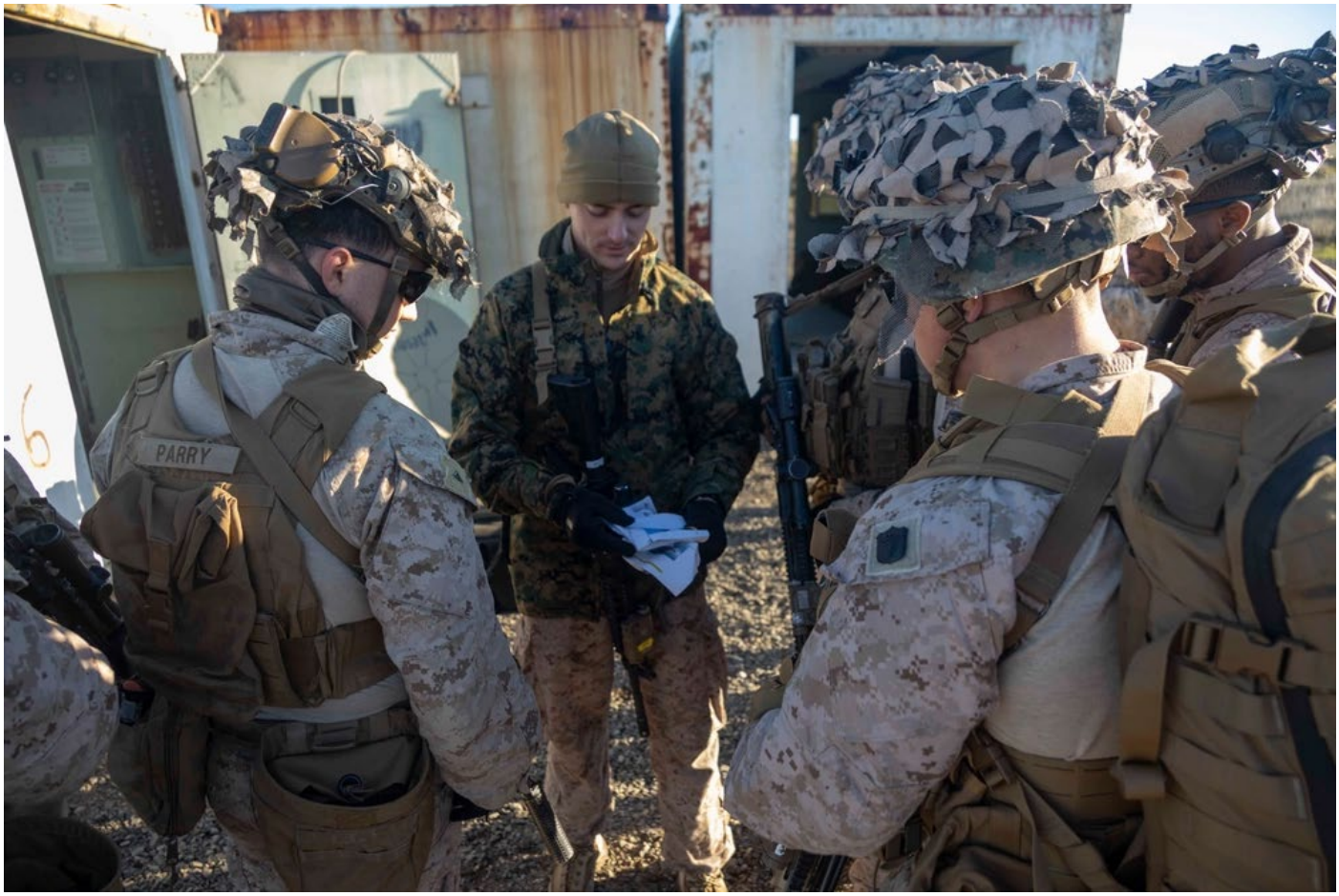
Next up… Post–World War I Reorganization of the Marine Corps

Intelligence Photographs in the News



CAMP LEJEUNE, NC, UNITED STATES
01.18.2024
Photo by Lance Cpl. Jack Labrador
II Marine Expeditionary Force

U.S. Marine Corps Lt. Col. Ruth Kehoe, off-going commanding officer of 2nd Intelligence Battalion (2nd Intel Bn), passes the colors to Lt. Col. Douglas McDonough, oncoming commanding officer of 2nd Intel Bn, during a change of command ceremony at Marine Corps Base Camp Lejeune, North Carolina, Jan. 18, 2024. The change of command ceremony symbolizes the passing of authority and responsibility from the off-going to the oncoming commanding officer. During the ceremony, Lt. Col. Ruth Kehoe relinquished command of 2nd Intel Bn to Lt. Col. Douglas McDonough. (U.S. Marine Corps photo by Lance Cpl. Jack Labrador)



SAN CLEMENTE ISLAND, CA, UNITED STATES

01.10.202 **SAN CLEMENTE ISLAND, CA, UNITED STATES**

U.S. Marines and Sailors assigned to the 15th Marine Expeditionary Unit receive an intelligence collections update prior to a patrol on San Clemente Island, California, Jan. 10, 2024. The Marines were patrolling an expeditionary advanced base site, which had been established to sense for nearby threats and build maritime domain awareness during the 15th MEU's integrated training with the Boxer Amphibious Ready Group. Expeditionary advanced base operations are a form of expeditionary warfare that allows Marines to operate from austere locations ashore or inshore within potentially contested maritime areas in order to enable fleet sustainment, conduct sea denial, or support sea control missions. (U.S. Marine Corps photo by Gunnery Sgt. Antonio Campbell)

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.