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 3 · Nov 2017

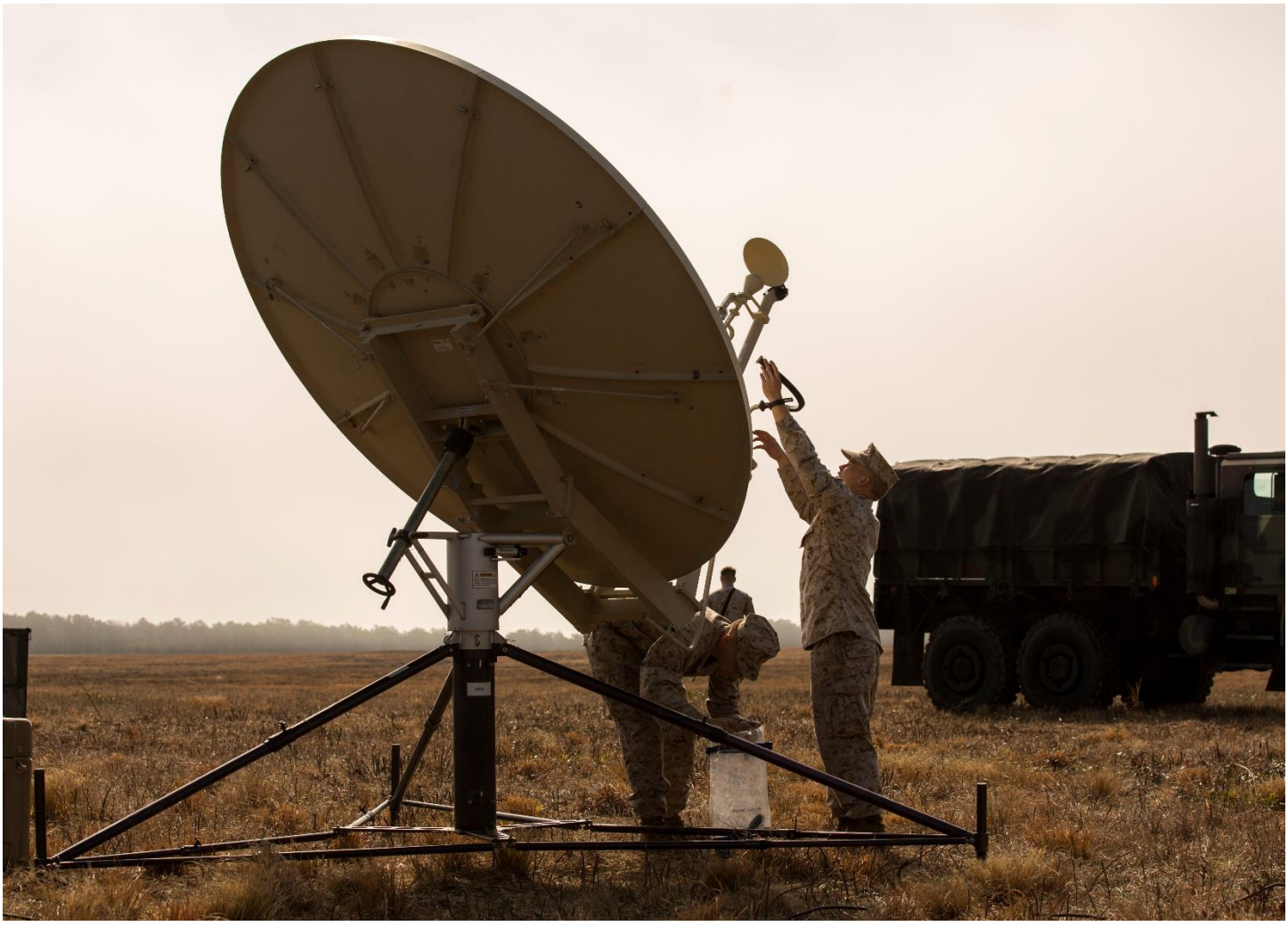


Photo By: Cpl Justin Updegraff

IN THIS ISSUE: FEATURE ARTICLE – MARINES, USBP TEAM UP TO PROTECT THE BORDER

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:

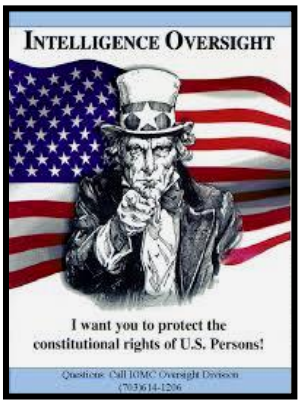
Director, Intelligence Oversight
Inspector General of the Marine Corps
Headquarters U.S. Marine Corps
701 South Courthouse Road
Building 12, Suite 1J165
Arlington, VA 22204

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

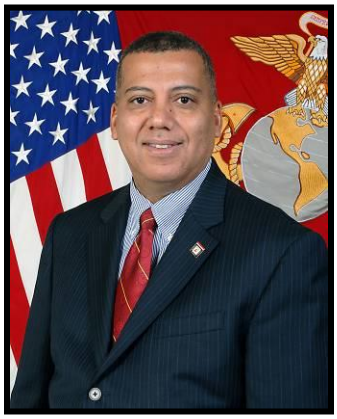
Naval Inspector General
http://www.ig.navy.mil/

Message from the Director, Intelligence Oversight

This edition of Overwatch is the latest of calendar year 2017. The caliber of Marines in the intelligence realm continues to set the standard as I conduct inspections throughout the fleet.

Our feature article was written by Cpl. Brianna Gaudi and discusses the use of Marine Corps personnel as part of the team working with the US Border Patrol. This is significant since the border issue was a highlight of the rhetoric during the last Presidential election. As usual, Marines are at the forefront.

Mark Pomerleau, wrote our second article about the vision of Brigadier General Henry, Director of Intelligence for the US Marine Corps and what he sees as significant requirements for Marine Corps intelligence to win on the battlefield in the future. .



In the third article, we look at the impact of banning Kaspersky, a leading Cyber Security software company from government wide contracts and the impact to the commercial product lines found in most homes and businesses.

The last article discusses the DOD Inspector General's report regarding the allegation of distorted intelligence reporting on ISIS.

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

Marines, USBP Team up to Protect Border

By Cpl Brianna Gaudi
II Marine Expeditionary Force

Marines with 2nd and 3rd Intel Battalion, Ground Sensor Platoon, under tactical control of Joint Task Force North, work in support of the U.S. Border Patrol in detecting, identifying, and alerting USBP of potential narcotics smuggling, human trafficking and illegal personnel.

Working in conjunction with the U.S. Border Patrol, the primary mission is to detect transnational threats to the homeland in order to prevent terrorists' weapons, including, weapons of mass destruction, from entering the United States.

Several drug trafficking organizations smuggle high volumes of illegal narcotics from Mexico to the United States for mass distribution. Drug smugglers use the heavy vegetation of to avoid surveillance and observation from U.S. Border Patrol in an attempt to evade detention and processing.

When apprehended by USBP, undocumented aliens or UDAs are processed and then are transferred to other government agencies for final disposition such as release with court date or deportation. In cases where drugs are involved, the drugs are confiscated and handed over to the Drug Enforcement Agency for proper disposal.

Having the Marines there provides a second set of eyes to support the mission. Marines place these sensors along the border in areas of interest known to be popular for crossing.
"These sensors allow the border patrol agents to cover more territory with fewer personnel, allowing them to capture UDA's and Drug Trafficking Organizations personnel smuggling narcotics from Mexico into the U.S.," said Col. Russ Draper, the Regional Support Team Chief, Joint Task Force North. "The Marines are providing a valuable service by helping to increase the capacity to secure the border."

Another device Marines use is an imager, which set up similar to a sensor, is not easily detected. Unlike a sensor, when the imager is activated it captures a picture which can make for easy identification of traffickers.

"The Marine Corps is providing a unique capability that not many organizations have," Draper said. "Their professionalism and behavior is impacting JTF-N and enhancing the relationships with the partners they work alongside."

Marines rotated 12 or 24 hour duty evolutions depending on the station they were at. During their duty, Marines watched for activations and when they saw something suspicious they would call it in to the Border Patrol, who would relay the message to agents they have in that area to investigate.

The set-up of some of the stations allowed the Marines to work side-by-side with the Border Patrol agents, but for other stations it is important they maintained good communication with each other. With good cooperation, it makes working together easier and allows the group to achieve their common goal.

"It's been a lot of fun, and is really cool to work with another government agency," said a tactical remote sensor systems technician with 3rd Intel Bn, GSP. "We learn a lot from each other which makes for a really good experience."

Working with the Border Patrol provided mutual benefits for the Marines. Not only were they able to help, but as a deployment they gained experience in handling and utilizing their equipment.

"We have been coming out here for several years now," said the section leader with 2nd Intel Bn,

GSP. “It’s a great way to employ our gear and get real-world training. You can’t recreate this kind of environment and it allows us to test all our capabilities with our equipment.”

In past years, the Marines had supported a two-month mission where they would spend only a little time at each station before moving on to the next. This year’s mission enabled them to bring more gear and cover a greater expanse of the border so they could monitor all stations for the entire operation.

“We love supporting the Border Patrol and want to catch the illicit activity that comes across just as much as they do,” said the section leader with 2nd Intel Bn, GSP. “The mission allows us to support the Border Patrol for an extended period of time without losing coverage along the border.”

With great success during the operation, the Marines have high hopes of returning in the upcoming years.

“We all play a really pivotal role here and we work well together,” said a tactical remote sensor systems technician with 3rd Intel Bn, GSP. “I believe we’ll have a lot of success in the future.”

Three Pressing Requirements for Marine Corps Intelligence

By Mark Pomerleau
C4IST Net
August 16, 2017

As the military pushes ahead in an increasingly complex and uncertain world, the battlefield of the future will necessitate certain capabilities to fight and win in the information age.

Brig. Gen. Dimitri Henry, Director of Intelligence for the Marine Corps, outlined three things he believes are needed from industry and academic partners to help the service in this future fight.

The first is an agile network, Henry said at the DoDIIS Worldwide Conference, detailing the mobility of Marines and the necessity of a network that can follow them in austere and expeditionary locations. They need information systems and data repositories — be they local or forward-deployed servers or the cloud — to move in the cyber and physical space in which Marines operate, he said.

Secondly, Henry called for resiliency and data integrity. “We get up close and personal with our adversaries, and we have data at rest around our formations,” he said.

The Marines need the “resiliency and data integrity” to make sound and timely decisions at the lowest level, he added. Marines fighting at the fire team level may be incapable of operating if the environment continues down its current path, he noted.

He emphasized that without this, Marines won’t be equipped, trained or educated on the network and the data needed for decision-making at the lowest levels.

Lastly, Henry said the force requires redundancy, not just in systems but in the ability to act as an enterprise. This includes the Marine Corps intelligence enterprise, the Defense Department’s information enterprise and the broader intelligence community.

Kaspersky Axed From Government wide Contracts

By Adam Mazmanian
FCW
July 12, 2017

Cybersecurity software from Russian vendor Kaspersky Lab is no longer available to federal agencies via the largest civilian acquisition contract vehicles, after a review by the White House, the General Services Administration and intelligence agencies.

NASA's Solutions for Enterprise-Wide Procurement contract vehicle and GSA's Schedule 70 have

dropped Kaspersky from their list of preapproved vendors out of a concern that the company could become a vector for Russia to attack federal networks.

"GSA's priorities are to ensure the integrity and security of U.S. government systems and networks and evaluate products and services available on our contracts using supply chain risk management processes," a GSA spokesperson told FCW in an emailed statement

Joanne Woytek, NASA SEWP program manager, said, "NASA has collaborated and coordinated with [the Office of Management and Budget], GSA and other government agencies on removal of Kaspersky Lab products from the SEWP contracts."

The move comes after a review that included intelligence chiefs. Adm. Mike Rogers, director of the National Security Agency and Cyber Command leader, told a Senate committee in May that he was "personally involved" in the Kaspersky review. Under questioning, the heads of five intelligence agencies including the CIA said they would not be comfortable using Kaspersky products on their networks.

The ban also applies to Schedule 67, GSA's photographic equipment and related supplies and services vehicle.

The Senate version of the 2018 defense bill currently under consideration includes a blanket ban on the use of Kaspersky products.

Kaspersky Lab denies that it represents any kind of threat or has any connection to the Russian government.

"Kaspersky Lab has no ties to any government, and the company has never helped, nor will help, any government in the world with its cyberespionage efforts. The company has a 20 year history in the IT security industry of always abiding by the highest ethical business practices and trustworthy development of technologies, and Kaspersky Lab believes it is completely unacceptable that the company is being unjustly accused without any hard evidence to back up these false allegations," the company said in a statement supplied to FCW.

The company noted that it has offered to provide its source code for an audit and make its CEO available for congressional testimony and meetings with government officials.

According to a July 11 Bloomberg Businessweek article citing internal company emails, Kaspersky has designed cybersecurity software to deflect distributed denial-of-service attacks and also deliver to Russian law enforcement the location of possible hackers. The report also alleges that Kaspersky supplies personnel to accompany Russian intelligence and police on raids and arrests. In a press release disputing some of the allegations in the article, Kaspersky noted that employees "might ride along to examine any digital evidence found, but that is the extent of our participation" in Russian police activity.

Kaspersky has a fairly limited profile in the federal space as a contractor. Its products are in use or have been used at the Bureau of Prisons, the Consumer Product Safety Commission and the Comptroller of the Currency at Treasury, but overall spending on the company's products by the federal government is far below $1 million, according to contracting data. The company's products do not appear on GSA's Continuous Diagnostics and Mitigation vehicle, a set of tools and services from vendors vetted by the Department of Homeland Security to provide cybersecurity services to federal agencies.

On the other hand, Kaspersky antivirus solutions are integrated in a range of routers, chip and software products from such household names as Cisco, Juniper, D-Link, Broadcom, Amazon and Microsoft.

"I don't always know what's in the box," one federal information security official told FCW. "The embedded technologies is what we have to figure out -- is it or is it not a problem," the official said.

Bloomberg Businessweek reported that $374 million of Kaspersky's $633 million in sales in 2016

were from the U.S. and Western Europe, and concerns that the firm has links to Russian intelligence could certainly dent Kaspersky's reputation.

Kremlin spokesperson Dmitry Peskov told reporters on a conference call that the move to block Kaspersky was political, according to a Reuters report.

"This is an absolutely commercial company which provides commercial services which are not only competitive but are super-competitive globally," Peskov said.

This isn't the first time lawmakers and policymakers have gone after foreign IT out of supply chain concerns. Chinese hardware and telecom vendors were the target of an effort in 2013 that resulted in restrictions on certain agencies acquiring tech from firms with strong ties to the Chinese government and military. While some restrictions were loosened, they remain on the books today.

IG: Military Did Not Distort Intelligence Reports on ISIS

By Deb Riechmann
Federal News Radio

WASHINGTON (AP) — A Defense Department review delivered to Congress on concludes that senior leaders at the U.S. Central Command did not exaggerate the progress the U.S. was making in fighting Islamic State militants, two U.S. officials said.

The long-awaited report from the Pentagon's inspector general is not expected to satisfy intelligence analysts who complained that officials were improperly reworking intelligence assessments being prepared for President Barack Obama and other top policymakers to offer a rosier view of U.S. operations against IS.

The probe began after at least one civilian analyst for the Defense Intelligence Agency told authorities he had evidence that officials at the Florida-based Central Command, which oversees operations in the Middle East, were improperly reworking the conclusions of these assessments.

A House GOP task force concluded in a report last year that there were "persistent problems" in 2014 and 2015 with the command's analysis of U.S. efforts to train Iraqi forces and fight IS in Iraq and Syria. The several hundred-page classified report, however, did not provide evidence that there were intentional efforts to distort intelligence analyses, said one U.S. official who had been briefed on the report.

While the report provided no evidence that IS intelligence assessments were altered, it did find that analysts' concerns were real and that if they didn't believe their work was being respected that sentiment could have affected the overall intelligence report, a second U.S. official said.

That official, who is familiar with the contents of the classified report, said the inspector general found no wrongdoing and no conspiracy or intent to color the intelligence, but concluded more broadly that there should be improvements in personnel management and leadership to address concerns by analysts about the treatment of their work.

As an example, the report notes that analysts who see their words being changed or left out of briefings could be less motivated to provide their best assessments. And if that sentiment made them less likely to bring up key points or conclusions, it affected the intelligence product, the official said.

The official said the report looked more broadly at the intelligence community as a whole and how it develops its assessments. And it said that by making people feel as though their work was not appreciated, there were unintended consequences, including that analysts may have left things out of their reports.

The official said there are no recommendations for anyone to be punished. But the report did include some recommendations that certain personnel develop better leadership skills. And the report talked at length about the need to improve processes

and the way the intelligence community works in order to make sure analysts are encouraged to bring their work forward.

The officials were not authorized to speak publicly about the report and demanded anonymity.

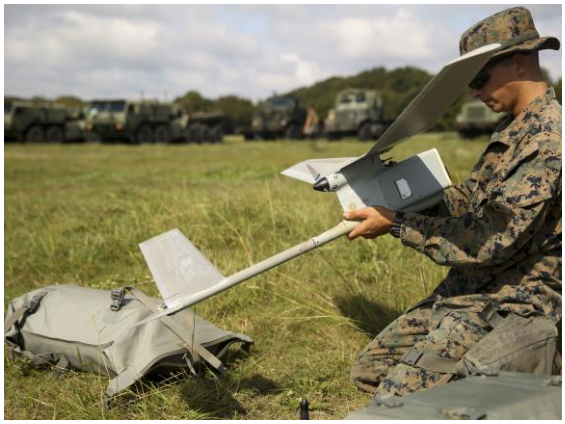
An unclassified version of the report is to be released on Wednesday.

In February 2016, the chairman of the House intelligence committee said the panel had been told that CENTCOM personnel had deleted files and emails amid the allegations that intelligence assessments were being altered. CENTCOM said that as a matter of policy, all senior leaders' emails were stored for record-keeping purposes and could not be deleted.

At the time, the chairman, Rep. Devin Nunes, R-Calif., also said the Office of the Director of National Intelligence had briefed the committee on a survey indicating that more than 40 percent of CENTCOM analysts believed there were problems with the integrity of the intelligence analyses and process.

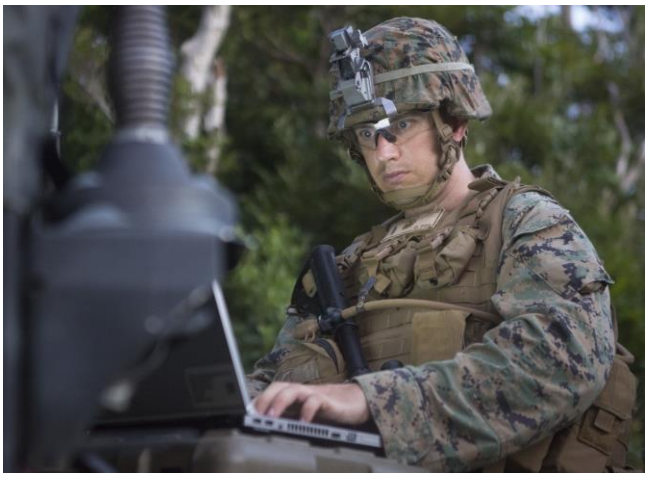
Each year the DNI conducts a survey at all 17 U.S. intelligence agencies to gain feedback on the integrity, standards and objectivity of the process used to analyze intelligence. A report on the survey issued in December 2015 indicated that 40 percent of those who responded at CENTCOM answered "yes" to the question: "During the past year, do you believe that anyone attempted to distort or suppress analysis on which you were working in the face of persuasive evidence?"

Intelligence Photographs in the News



MARINE CORPS BASE CAMP LEJEUNE, NC
Photo by Lance Cpl. Gloria Lepko
II Marine Expeditionary Force
A Marine constructs an intelligence collection device used to remotely photograph areas with minimal detection during a field training exercise at Camp Lejeune, N.C., Sept. 17-21, 2017. The field exercise prepares Marines for future deployments though events including engineer reconnaissance, helicopter operations, improvised explosive device lanes with route clearing courses, survivability tasks, breeching, and urban operations. The Marines are with 2nd Combat Engineer Battalion.

OKINAWA, JAPAN
Photo by Cpl. Carl King
3rd Marine Division
1st Lt. Christopher Anderson types up a detailed report during Combat Assault Battalion Field Exercise 17.4 September 12, 2017, on Camp Hansen in Okinawa, Japan. The purpose of FEX 17.4 is to prepare the battalion for combat operations while simultaneously conducting company level training consistent with company training plans and annual training requirements. Anderson is the battalion intelligence officer for Combat Assault Battalion, 3rd Marine Division, III Marine Expeditionary Force.



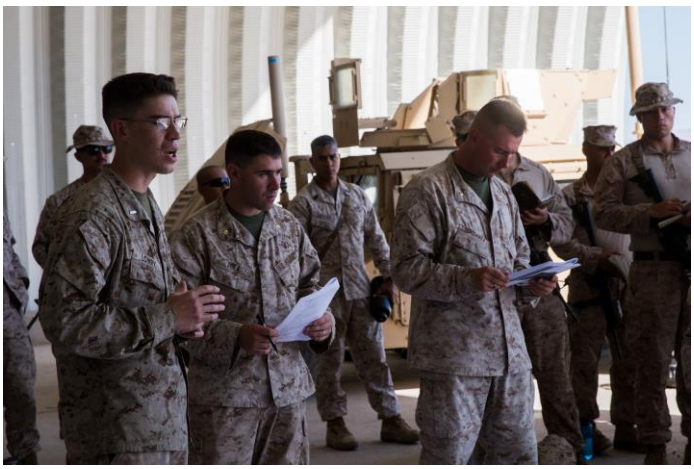


Photo by Cpl. Christopher Mendoza
2nd Marine Division
U.S. Marine Corps 1st Lt. Nathan Lowry, intelligence officer with Marine Air-Ground Task Force-8 (MAGTF) conduct a rehearsal of concept drill prior to executing an air assault during Integrated Training Exercise 5-17 (ITX) on Marine Corps Air Ground Combat Center Twentynine Palms, Calif., Aug. 9, 2017. The purpose of ITX is to create a challenging, realistic training environment that produces combat-ready forces capable of operating as an integrated MAGTF.

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, DoD_M 5240, 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 5000.34F

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.