



# 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 2 · Issue 1 · April 2009



**IN THIS ISSUE:** Feature Article – Intelligence Oversight-Regulation Not Prevention



## Inspector General of the Marine Corps

*The mission of the Inspector General of the Marine Corps is to promote Marine Corps combat readiness, integrity, efficiency, effectiveness, and credibility through impartial and independent inspections, assessments, inquiries, and investigations*

## 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  
FOB#2 Navy Annex, Rm 2234  
Washington, District of Columbia 20380-1775

### Intelligence Oversight Division Staff

GS15 Edwin T. Vogt, Director  
LtCol Steven P. Manber, Deputy Director  
LtCol Richard S. Martindell, Sensitive Activities

# Inside This Issue

## Features

- 1 **Intelligence Oversight-Regulation not Prevention**
- 2 **Minimum Training Requirements**
- 3 **Helpful Hints**
- 4 **The Need for Records**
- 5 **Barriers to an Effective Program**
- 6 **Collection-A Practical Definition**
- 7 **Vision for National Intelligence**
- 8 **Training Scenarios**
- 9 **Intelligence Photographs in the News**



## Web Links

Assistant to the SECDEF for Intel Oversight (ATSD-IO)  
<http://www.defenselink.mil/attdio/main.html>

Marine Corps Inspector General  
<http://hqinet001.hqmc.usmc.mil/ig/>

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

# Message from the Director, Intelligence Oversight

I would like to thank all of you for your views and comments regarding this Intelligence Oversight journal. The comments I have received with regard to this effort have been extremely positive. In order to continue to provide the information on the most important and relevant oversight issues, I am requesting that our intelligence professionals submit ideas for future topics of interest that you feel would benefit the Marine Corps Intelligence Community as well as comments and feedback. Please provide them directly to my deputy at <mailto:steven.manber@usmc.mil>



I would like to welcome aboard Brigadier General Kenneth J. Lee as the new Inspector General of the Marine Corps. We at the IG look forward to supporting him to accomplish the mission as directed. BGen Lee is a former Hornet pilot and a member of the Virginia and DC bar. His expertise will be extremely valuable in his new role as IGMC. I would also like to announce that Col. Kimo Hollingsworth has moved on and taken a billet in Iraq and LtCol. Steven Manber has picked up the mantle as the new Deputy Director for Intelligence Oversight in his reserve capacity. LtCol Manber's civilian job is a Special Agent with the Defense Criminal Investigative Service and I look forward to working with him as my deputy.

In a Memorandum issued by the Director of National Intelligence and the Chairman, Intelligence Oversight Board since our last issue there has been a considerable change in Reporting Criteria with regard to Intelligence Oversight.

[EO 13462](#) tasks the Intelligence Oversight Board (IOB) with issuing criteria on the thresholds for reporting intelligence oversight matters to the IOB and to the Director of National Intelligence (DNI). It also tasks the DNI with issuing instructions relating to the format and scheduling of such reporting. The IOB continues to act as an independent entity appointed by the President to ensure that the Constitution and laws of the United States are respected and to report to the President in accordance with the functions assigned to the IOB by EO 13462.

To implement [EO 13462](#), the DNI will execute day-to-day intelligence oversight responsibilities. Among other things, this will include reviewing the guidelines by which Intelligence Community (IC) components report intelligence activities to ensure they are consistent with Part 1.7(d) of EO 12333 and with EO 13462, reviewing reports submitted to the IOB, and providing the IOB with a quarterly assessment of the content, quality, and timeliness of reporting by the IC.

I continue to be impressed at the professionalism and knowledge of our Intelligence Marines I meet as I travel around the fleet. Please continue to be engaged and keep up the great work.

**Semper Fidelis**  
**Edwin T. Vogt**  
**Director, Intelligence Oversight Division**  
**Office of the Inspector General of the Marine Corps**  
**Ph: 703-692-7445 DSN: 222-7445 Email: [Edwin.Vogt@usmc.mil](mailto:Edwin.Vogt@usmc.mil)**

# Feature Article

## Intelligence Oversight Regulation Not Prevention

The 11 September 2001 terrorist attacks on America presented the intelligence community with unprecedented challenges. Many of the perpetrators of these attacks lived for some time in the United States, and there is evidence that some of their accomplices and supporters may have been U.S. persons. This has raised many questions regarding intelligence collection authority.

Overall, there is no absolute ban on military intelligence components collecting U.S. person information. That collection, rather, is REGULATED by [Executive Order 12333](#), [DoD 5240.1-R](#) and for Marines, [MCO 3800.2B](#). In fact, intelligence components may collect U.S. person information when the component has the mission (or function) to do so, and the information falls within one of the categories listed in DoD 5240.1-R and MCO 3800.2B. The two most important categories are foreign intelligence and counterintelligence. Both categories allow collection about U.S. persons reasonably believed to be engaged, or about to engage, in international terrorist activities. Within the United States, those activities must have a significant connection with a foreign power, organization, or person (e.g., a foreign based terrorist group).

Some Services have received reports from the field of well intentioned military intelligence personnel declining to receive reports from local law enforcement authorities, solely because the reports contain U.S. person information. In fact, Military Intelligence (MI) may receive information from anyone, anytime. If the information is U.S. person information, MI may retain that information if it meets the two-part test – the unit has the mission/function to do so, and it falls within one of the categories listed in DoD 5240.1R and MCO 3800.2B. If the information received pertains solely to the functions of other DoD components, or agencies outside DoD, MI may transmit or deliver it to the appropriate recipients, per MCO 3800.2B.

Remember, merely receiving information does not constitute "collection." Overall, collection entails receiving "for use." Intelligence Oversight laws are designed to "regulate" collection, not ban or prevent collection.

## Minimum Training Requirements

Oversight training can take many forms, but there are certain minimum requirements that must be fulfilled. First, familiarity with the provisions of Executive Order 12333, DoD Directive 5240.1-R, and implementing instructions which apply to the Marine Corps (MCO 3800.2B). At a minimum, this entails an understanding of at least DOD Directive 5240.1-R procedures and those other procedures that pertain to activities performed by the unit. It should be emphasized in training that reporting questionable activities is mandatory, and no adverse action may be taken against Marines for reporting questionable activities.

## Helpful Hints

The standard training regimen for Intelligence Oversight (IO) training is to have Marines watch the annual standard IO video. The most current is a DIA production entitled "Intelligence Oversight." While this may fulfill the intent of the law, IG (IO) recommends that IO training be augmented with other types of training approaches. Overall, try and use a variety of awareness tools. Many organizations develop a slide presentation followed by a question and answer period; others have implemented computer-based training and/or testing. A highly effective approach is to conduct an actual case study review. If done properly, a good case study review can fulfill the IO requirement and also serve to fulfill a Professional Military Education requirement.

## Effective Intelligence Oversight The Need for Records

One of the best ways to ensure effective intelligence oversight is maintain written or electronic records of your training program and/or other activities. For many Marines, SOPs, turnover folders and training guides are routine. However, many of

these products are usually old, outdated or are incomplete. All effective IO programs should have established and maintained records to document when Marines have received training, and to provide a mechanism to assure that those Marines who missed training for operational or other reasons (e.g. leave, TDY) are trained at the earliest opportunity. Overall, written/electronic records ensure continuity between changes of command, changes of intelligence personnel and changes in billet/duty assignments.

### **Intelligence Oversight Barriers to an Effective Program**

One of the most significant constraints in commands being able to effectively identify and report intelligence oversight abuses is the very nature of intelligence work. Intelligence work is often laden with a high degree and pervasiveness of secrecy surrounding intelligence policy, information, activities, operations, resources, and personnel. The secrecy imperative results in a system that is often closed to outsiders – to include most members of a military command.

Overall, the restrictions and requirements to protect sensitive information, sources, and methods, will often slow or delay revelations about intelligence oversight violations. All of the checks and balances to ensure compliance with U.S. law is procedural – like any process, effectiveness ultimately requires active Command involvement, vigilance and training.

### **Collection – A Practical Definition**

One of the biggest hurdles in understanding intelligence oversight is a clear working definition of what collection really means. In general, information is “collected” when an intelligence person gathers or receives information in the course of official duties and the person intends to use the information for intelligence purposes. One of the underlying factors of defining “collection” is actions that demonstrate intent to use or retain the information. Examples include producing an intelligence information paper/briefing or incident report, or adding the information to an intelligence

database or intelligence files for reference or future use. Data acquired by electronic means is “collected” only when it is processed into intelligible form. Information held or forwarded to a supervisory authority solely for a collectability determination, and not otherwise disseminated within the intelligence component, is not considered “collected.” For more information on intelligence oversight definitions, refer to DoD 5240.1R – Procedures for Governing DoD Intelligence Components & U.S. Persons.

### **Vision for National Intelligence**

In October 2008, the Office of the Director of National Intelligence (DNI) released a new vision statement/document titled [\*Vision 2015: A Global Networked and Integrated Intelligence Enterprise.\*](#) According to the Office of the DNI, Vision 2015 expands upon the notion of an Intelligence Enterprise, first introduced in the National Intelligence Strategy and later in the 100 and 500 Day Plans. It charts a new path forward for a globally networked and integrated Intelligence Enterprise for the 21st century, based on the principles of integration, collaboration, and innovation. One of the challenges outlined in the document is the “blurring of lines that once separated foreign and domestic intelligence and the increase importance of homeland security.” The document also highlights that “we must also respect and maintain the privacy of civil liberties of all Americans.” The document can be located at [http://www.dni.gov/Vision\\_2015.pdf](http://www.dni.gov/Vision_2015.pdf) on the world-wide-web.

### **Training Scenarios Intelligence Oversight Related to CONUS Antiterrorism/Force Protection**

This information is provided to assist commands in determining what role military intelligence can play to support the commander specifically in providing intelligence on the current international terrorism threat to our forces, property and installations within the continental United States (CONUS). But, before we launch into the subject of Intelligence Oversight related to CONUS antiterrorism/force

protection a few preliminary questions must be posed and answered.

#### Scenario #1

While deployed ISO Dynamic Mix and through local liaison, the command becomes aware of a U.S. citizen associated with the Basque Separatists who are suspected to be observing the unit's activities. This person has further been identified as developing relationships with command members on liberty. The command S-2 has developed a portfolio on the individual through interview, research and liaison.

IAW Procedure 2, information about U.S. persons may be collected when: (a) The person is reasonably believed to be engaged in intelligence activities on behalf of a foreign power, or international terrorist activity and (b) When the information is needed to protect the safety of persons or an organization.

However, such collection must be lawful and when possible use the least intrusive means available.

Additional restrictions apply when the collection occurs within the U.S. Although the command may not have violated intelligence oversight regulations, they have exceeded their authority in the active collection of information.

---

#### Scenario #2

While exploiting an ATARS image for training value, the command observes a camouflaged area with many cars. You recall a friend telling you about a car that was stolen from her. Can you provide this imagery to LE? Can you inspect this image for your friend's car? Can you retain the image for training value?

Procedure 12 authorizes the sharing of information incidentally obtained, during authorized activities with local, state, or federal Law Enforcement (LE) agencies as appropriate. You may report this information to LE but should coordinate with NCIS first. However, to further inspect the image (an 0241 function) when it is reasonably expected to reveal U.S. persons information may be inappropriate. SJA review should be obtained first. There may be a LE need for expert assistance in exploiting the imagery. Providing this type of assistance is restricted to support for federal agencies. When lives are in immediate danger, this specialized assistance may be extended to state or local LE. Retaining this image for training value when it represents private property or U.S. person's information, would be a violation of applicable domestic imagery policies and intelligence oversight regulations unless permission was received from the owner to retain for training purposes.

---

#### Scenario #3

A command member is interested in some property for sale in the vicinity of a scheduled flight path. He requests the air crew to make a small deviation and obtain imagery of the property for him.

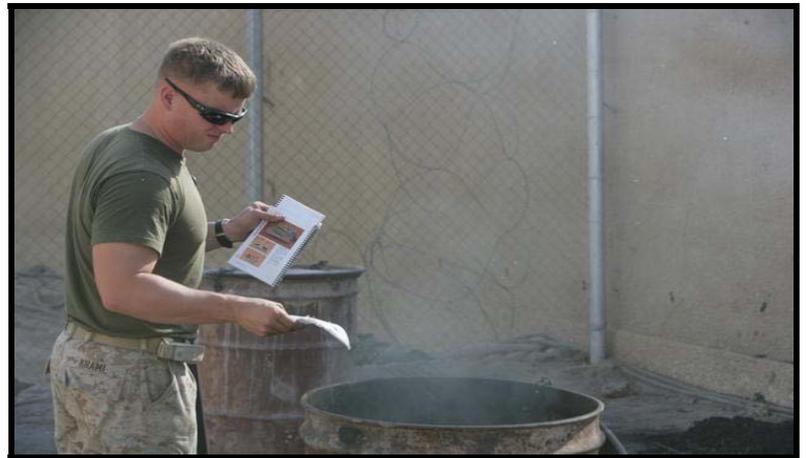
This is an inappropriate use of specialized equipment and an unauthorized collection of domestic imagery. The property to be imaged is private property and this action constitutes a direct violation of intelligence oversight, in that U.S. persons are not to be specifically targeted by overhead reconnaissance. This is also a violation of USMC and Domestic Imagery Policy by deviating from an authorized flight plan and approved domestic imagery collection. Furthermore, there is a violation of Joint Ethics Regulations regarding the use of Government property.

## *Intelligence Photographs in the News*



U.S. Marine Corps Maj. Gen. John F. Kelly, commanding general, I Marine Expeditionary Force, attends an intelligence briefing at Forward Operating Base Sykes, Nineveh, Iraq, Jan. 9, 2009. U.S. Marines and Iraqi soldiers are meeting with border enforcement agents to discuss regional security issues. (U.S. Marine Corps photo by Lance Cpl. Lindsay L. Sayres/Released)

1/3/2008 - U.S. Marine Lance Cpl. Craig A. Kramel, assigned to 2nd Intelligence Battalion, throws documents into a burn can for destruction on Camp Fallujah, Iraq. (U.S. Marine Corps photo by Sgt. Jeremy M. Giacomino/Released)



10/09/2008 - Iraqis gather around U.S. Marines assigned to Golf Company, I Marine Headquarters Group during a patrol through a village near Camp Fallujah, Iraq, Oct. 9, 2008. The Marines are conducting the patrol to maintain security, gather intelligence and distribute supplies to area villages. (DoD photo by Lance Cpl. Lindsay L. Sayres,

# 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**

- 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, E.O.12334, DoD Dir 5240.1, DoD Reg 5240.1-R, SECNAVINST 3820.3, MCO 3800.2
- 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 5000.34D](#)
- 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 5000.34D](#)
- 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.
- QUESTIONABLE ACTIVITIES:** Any conduct that may constitute a violation of applicable law, treaty, regulation or policy.