



Intelligence Oversight

January 2008

JOURNAL OF THE MARINE CORPS INTELLIGENCE OVERSIGHT DIVISION

Volume I · Issue 1 · January 2008



IN THIS ISSUE: Feature Article – Successful Intelligence Oversight Training



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.

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/>

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 Kimo Hollingsworth, Deputy Director-0202
LtCol Richard S. Martindell, Sensitive Activities, 5803

Inside This Issue

Features

- 1 **Successful Intelligence Oversight Training**
- 2 **Foreign Intelligence Surveillance Act**
- 3 **Worldwide Intelligence Oversight Conference**
- 5 **Frequently asked questions**
- 4 **Intel Photos in the News**

Message from the Director, Intelligence Oversight

Welcome to the first Intelligence Oversight Newsletter from the Office of the Inspector General. The intent is to broaden the awareness of Marine Corps intelligence professionals of their responsibilities under current Executive Orders and Directives within the Marine Corps and the Department of the Navy.

The Global War on Terrorism has generated considerable debate about the role of intelligence and intelligence oversight within the Intelligence Community (IC), the Department of Defense (DoD), Congress, and more importantly, the general public. From the outset, the term “oversight” is vague, and when associated with intelligence, it is often misconstrued and viewed negatively. In effect, intelligence oversight is the internal and external management controls (checks and balances) we use to ensure that we conduct our intelligence activities effectively and within legal and policy boundaries. Some methods we use in the Marine Corps are in the establishment of clear policies and directives, and by ensuring proper training and awareness programs are in place through visits, assessments and inspections.



The Department of Defense (DoD) Intelligence Oversight (IO) program came about as a result of certain activities conducted by DoD intelligence and counter-intelligence units against U.S. Persons involved in the Civil Rights and anti-Vietnam War movements. During the 1960s and 1970s, the United States experienced significant civil demonstrations from protesters associated with these movements. Some of these demonstrations were believed to be beyond the ability of civilian authorities to control, and military forces were used to assist in the restoration of order. Units deploying for this purpose discovered they needed basic pre-deployment intelligence to perform their missions. The Army, designated as executive agent for providing aid to civilian authorities, requested assistance from the Federal Bureau of Investigation (FBI). When the FBI was unable to provide the information needed, the Army began collecting information on U.S. citizens.

Over time, this collection mushroomed and led to abuse of the Constitutional rights of our citizens. Eventually, DoD intelligence personnel were using inappropriate clandestine and intrusive means to collect information on the legitimate political positions and expressions of U.S. Persons. When this became public, Congress conducted special inquiries and eventually created intelligence oversight committees. As a result, the President established executive orders for the proper conduct of intelligence activities.

Traditionally, our nation has separated the functions of law enforcement and foreign intelligence collection between agencies operating domestically and those operating overseas. These are important distinctions that not only apply to geographic boundaries, but also extend to the status of individuals, mainly U.S. Persons. Intelligence oversight provides guidance and supervision to ensure intelligence and counterintelligence personnel do not collect, retain or disseminate information about U.S. Persons unless performed in accordance with specific guidance, proper authorization and only within specific categories. These issues are complex because the rules and procedures are strict and the definition of U.S. Persons is broad. Despite the complexity, intelligence oversight is every Marine’s responsibility and we want to ensure proper intelligence oversight training of all intelligence personnel and operational leaders who direct intelligence activities. It will ultimately protect you, your Marines and the Marine Corps as an organization.

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

Feature Article

Successful Intelligence Oversight Training

Intelligence oversight training is an annual requirement for intelligence Marines. In addition, it is normally conducted as part of pre-deployment training for intelligence personnel. Recent trends suggest that intelligence oversight training is often ignored or pushed aside in order to meet “higher priority” training requirements. This trend represents a “slippery slope” that may ultimately lead to violations of the law and unwanted public scrutiny of Marine Corps intelligence.

Intelligence oversight is the process of ensuring that all DoD intelligence, counterintelligence, and intelligence related activities are conducted in accordance with applicable U.S. law, Presidential Executive Orders, and DoD directives and regulations. Like all successful training, fundamental leadership by the unit commander sets the standard and the level of emphasis. If it is important to the commander, then it will be important to the Marines. There is no substitute for command involvement – it is the basic foundation for any successful training program.

In most commands the basic responsibility for intelligence oversight will naturally fall within the responsibility of the S-2/G-2. This appointment should be in writing and with formal notification/counseling. Overall, a good oversight training program involves the command at all levels. Intelligence and security should be an ongoing process and constant vigilance is prudent, regardless of the military occupational specialty. It will also reinforce the concept that “every Marine is a collector.”

In addition, there should be a periodic review of command activities and programs to ensure the oversight program is compliant with current laws and directives. Since September 11, there have been several important revisions, updates, and also new guidance/clarification on intelligence activities related to anti-terrorism/force protection, domestic

urban training, use of the internet, and domestic imagery.

Like any training program, Marines should identify potential issues and determine a way ahead to mitigate future problems and set a path for future lawful conduct. In so doing, it is highly recommended that the unit Staff Judge Advocate be involved in training. This is especially true for training exercises and real-world operations conducted in CONUS or where U.S. Persons could be targeted for collection.

The bottom line is that intelligence oversight is often overlooked until something goes wrong. Simply put, intelligence oversight training is designed to protect you and your Marines.

Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) of 1978 is a U.S. federal law prescribing procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between or among "foreign powers."

In 2004, FISA was amended to include a "lone wolf" provision that amended the definition of "foreign power" to permit the FISA courts to issue surveillance and physical search orders without having to find a connection between the "lone wolf" and a foreign government or terrorist group. A “lone wolf” is considered a non-US person who engages in or prepares for international terrorism.

Public knowledge about FISA became widespread in 2005 following reports in the media that revealed the National Security Agency monitored and tracked phone calls originating from or going to some countries of interest. Overall, the statute limits its application to US Persons. A US person includes citizens, lawfully admitted permanent resident aliens, and businesses incorporated in the US.

More recently, the issue has received considerable attention because President Bush asked Congress to reform the FISA in order to ease restrictions on surveillance of terrorist suspects where one party (or both parties) to the communication are located overseas. In August 2007, the House and the Senate

both passed, and the President signed, The Protect America Act of 2007 (Public Law 110-55).

Under the Protect America Act of 2007, communications that begin or end in a foreign country may be wiretapped by the US government without supervision by the FISA Court. The Act removes from the definition of "electronic surveillance" in FISA any surveillance directed at a person reasonably believed to be located outside the United States. As such, surveillance of these communications no longer requires a government application to, and order issued from, the FISA Court.

The code defines "foreign intelligence information" as information necessary to protect the United States against actual or potential grave attack, sabotage or international terrorism. The Act permits electronic surveillance without a court order for the period of one year provided it is only for foreign intelligence information; targeting foreign powers as or their agents; and there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.

The government may also seek a court order permitting surveillance from the FISA court. Approval of a FISA application requires that the court find probable cause that the target of the surveillance is a "foreign power" or an "agent of a foreign power", and that the places at which surveillance are requested are used or will be used by that foreign power or its agent. In addition, the court must find that the proposed surveillance meet certain "minimization requirements" for information pertaining to US Persons.

In addition to electronic surveillance, FISA permits the "physical search" of the "premises, information, material, or property used exclusively by" a foreign power. The requirements and procedures are nearly identical to those for electronic surveillance.

A law passed in August, the Protect America Act, revised the 1978 Foreign Intelligence Surveillance Act procedures to better deal with modern communications and technology. That law will expire at the end of this month.

NORAD NORTHCOM Host the First Worldwide Intelligence Oversight

Conference Excerpt by Armando Carrasco, JTF North Public Affairs

In its continuing effort to ensure compliance with the DoD Intelligence Oversight program (IO), North American Aerospace Defense Command and U.S. Northern Command sponsored the 1st Annual World-Wide Intelligence Oversight Conference Dec. 4-6 at Joint Task Force North Headquarters on Fort Bliss, Texas.

“The events of September 11th, 2001 brought to our nation a threat that requires all elements of national power to defeat. It caused us in the business of providing for the security and defense of the nation an urgent need to find new ways to work together to confront the threat of terrorism to the homeland” said Joint Task Force North Commander, Brig. Gen. Anthony R. Ierardi. JTF North is the USNORTHCOM unit tasked to provide military support for homeland security to the nation’s federal law enforcement agencies.

“As a result of the greater need to develop information and to share it between agencies, there needs to be a continuous assessment and collaboration among the operational, intelligence and legal mechanisms to ensure that we continue to unquestionably protect the constitutional rights of U.S. Persons,” said Ierardi.

DoD intelligence personnel engaged in any intelligence activity (e.g. collection, research, analysis, production, retention, or dissemination) as well as all non-intelligence personnel assigned to a DoD intelligence unit, must be familiar with the provision of IO policies and instructions. Contractors performing intelligence or counterintelligence work for DoD intelligence or counterintelligence organizations have the same IO responsibilities as government civilian and military personnel.

Conference events included panel discussions, presentations and working group participation: special emphasis was given to current IO issues and future applications of policy pertaining to the evolving nature of technology and interagency cooperation in today’s operational environment.

Frequently Asked Questions

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.

Q1. What is Intelligence Oversight and what is the purpose of the Department of Defense Intelligence Oversight program?

A1. Intelligence Oversight is the process of ensuring that all DoD intelligence, counterintelligence, and intelligence related activities are conducted in accordance with applicable U.S. law, Presidential Executive Orders, and DoD directives and regulations. The DoD Intelligence Oversight program has two main objectives. The program is designed to ensure that the DoD can conduct its intelligence and counterintelligence missions while protecting the statutory and constitutional rights of U.S. persons. (Basic references: Executive Order 12333, DoD Regulation 5240.1-R, SECNAVINST 3820.3E, and MCO 3800.2B)

Q2. What is the difference between the terms "U.S. persons" used in Intelligence Oversight references and "U.S. citizens?"

A2. The term "U.S. persons" includes U.S. citizens, but is broader. It also includes permanent resident aliens, unincorporated associations substantially composed of U.S. citizens or permanent resident aliens, and corporations incorporated in the U.S. and not directed and controlled by a foreign government.

Q3. Do Intelligence Oversight laws and regulations apply today under the current international terrorist conditions with the attacks on U.S. territory?

A3. Yes. While the Executive and Legislative branches are reported to be reviewing Intelligence Oversight policies, current rules remain in place. We will ensure

any changes in policy are disseminated in a timely manner.

Q4. My CONUS commander wants my intelligence unit/section to provide intelligence in support of his antiterrorism/ force protection mission. May I do this?

A4. This question requires a lot of qualifications to any answer. **Generally speaking you may support your commander with foreign intelligence on non-U.S. persons, but not with intelligence on any U.S. persons.** SECDEF message, DTG 181700Z Nov 98 provides further clarification on this particular subject.

1. When **foreign groups or persons** threaten DoD personnel, resources, or activities – whether CONUS or OCONUS – DoD intelligence/ counterintelligence components may intentionally target, collect, retain, and disseminate information on them (unless the groups or persons in question meet the definition of "U.S. persons" provided above). For example, you may collect and retain information on Osama bin Laden and associates whether CONUS or OCONUS if they are not "U.S. persons."

2. **Generally you may not intentionally target, collect, retain, and disseminate information on U.S. persons whether CONUS or OCONUS.** Information pertaining to U.S. persons, which poses a threat to DoD personnel, resources, or activities, falls under the realm of law enforcement and security. As such, DoD law enforcement and security organizations, as opposed to intelligence/counterintelligence components, may legally accept and retain such information for up to 90 days, unless longer retention is required by law or permission is specifically granted by SECDEF (DoDD 5200.27). An S-2 section in a standard infantry battalion may not, for example, collect and retain information (to include publicly available newspaper clippings or internet articles) on Osama bin Laden's relatives or associates whether CONUS or OCONUS if they are "U.S. persons."

3. **Exceptions** exist which allow intelligence/ counterintelligence components to intentionally target, collect, retain, and disseminate information on U.S. persons. For example, if you are assigned to, or in support of, a DoD law enforcement organization or unit with a specific security mission, you may collect information on domestic threats to DoD that are "reasonably believed" (not a "gut feeling" or hunch, but reason that can be articulated) to have a foreign connection. **Even under these circumstances, you are limited to the 13 categories of information laid out in Procedure 2 of DoD Regulation 5240.1-R.** Under such conditions you should closely coordinate with law enforcement to provide and receive needed information.

With question 4 asked and answered, some further clarification and guidance is necessary. The FBI has the lead when it comes to antiterrorism information INCONUS. NCIS is our Marine Corps main source and support in this arena. This usually occurs via the operational antiterrorism/force protection and/or military law enforcement channels. Commanders should take advantage of law enforcement liaison activities to monitor criminal activity in the vicinity of their installations/activities. Acts of terrorism and threats to harm personnel or destroy Government property are criminal acts.

Q5. May I disseminate U.S. person information?

A5. Any information, which is legally collected and retained, may be disseminated to other government agencies that have a need to know.

Q6. May my unit circumvent the restrictions imposed by DoD Regulation 5240-1-R by having contractors perform the tasks that we as government personnel are not permitted to do?

A6. No. The Government may not hire contractors to do things that are improper or illegal.

Q7. The FBI has asked me to provide an interpreter to assist in interviewing an alien. May I do so?

A7. Provision of expert support by intelligence professionals to law enforcement agencies is permitted (see DoD Regulation 5240.1-R, Procedure 12) **providing** your command structure and general counsel/staff judge advocate concur. Any such requests from any organization outside of the Marine Corps must be routed through proper channels to Headquarters Marine Corps, Manpower and Reserve Affairs. Your interpreter should not bring back to your DoD facility any information obtained in the interview nor should this information be included in any DoD database.

Q8. I'm an intelligence/counterintelligence officer assigned to another Service, a Joint Command, federal agency, or NATO organization. Do Intelligence Oversight rules apply to me?

A8. Yes, they do. Executive Order 12333 and pertinent implementing directives and regulations still apply. You are required to follow all Intelligence Oversight rules.

Q9. Do other agencies in the Intelligence Community besides DoD have to follow Presidential Executive Order 12333? Do they have Intelligence Oversight programs?

A9. Yes. Presidential Executive Order 12333 applies to the entire Executive Branch. All departments and agencies that conduct intelligence or counterintelligence activities must implement Intelligence Oversight programs.

Q10. Where do I go with other questions on Intelligence Oversight issues?

A10. Call the Inspector General of the Marine Corps, Oversight Division at (703) 614-1206, Ext 164 with your questions

The Intel Community



U.S. Marine Corps Brig. Gen. John R. Allen, deputy commanding general of Multi-National Force-West, discusses an issue with the Tribal Engagement Officer in Charge and a Human Exploitation Team Specialist -10 June 6, 2007 in An Nukhayb, Iraq. (Released to Public)

Joint Task Force North Deputy Director for Intelligence, Gabe Reyes on right, leads a working group discussion on Intelligence Oversight. The group focused on current IO issues and future applications of policy pertaining to the evolving nature of technology and interagency cooperation (Released to Public)



U.S. Navy Sailors and Marines of the Navy and Marine Corps Intelligence Center (NMITC) conduct training exercises July 20, 2007, in an area of Virginia Beach, Va., designed to simulate conditions in Iraq and Afghanistan. The NMITC facility at Naval Air Station Oceana, Dam Neck Annex is designed to teach Sailors and Marines to use non-traditional intelligence collection efforts to combat a non-traditional enemy. (U.S. Navy photo by Mass Communication Specialist 2nd Class Jason R. Zalasky) (Released) (Released to Public)