UNITED STATES ARMY INSPECTOR GENERAL SCHOOL

INTELLIGENCE OVERSIGHT GUIDE

DEPARTMENT OF THE ARMY INSPECTOR GENERAL AGENCY
TRAINING DIVISION
5500 21ST STREET, SUITE 2305
FORT BELVOIR, VIRGINIA 22060-5935
November 2014

DEPARTMENT OF THE ARMY
OFFICE OF THE INSPECTOR GENERAL
1700 ARMY PENTAGON
WASHINGTON, DC 20310-1700

SAIG-TR

MEMORANDUM FOR ALL U.S. ARMY INSPECTORS GENERAL

SUBJECT: *The Intelligence Oversight Guide*

1. *The Intelligence Oversight Guide* represents U.S. Army Inspector General (IG) doctrine for the planning, execution, and completion of all Army IG Intelligence Oversight inspections. This doctrine is authoritative and has the backing of Army IG policy in the form of Army Regulation 20-1, *Inspector General Activities and Procedures.* All IGs will employ this doctrine within the policy framework set forth in Army Regulation 20-1. If a discrepancy exists between the guide and the regulation, the regulation will take precedence.

2. This doctrinal guide's Foreign Disclosure Determination / Designation is FD-1 (as of 19 June 2015), which means that this doctrine is releasable to members of partner nations and to the general public.

3. If you have questions or comments about this guide, or identify discrepancies or inconsistencies requiring attention, please contact Mr. Stephen M. Rusiecki, Dean of Academics and Deputy Commandant, U.S. Army Inspector General School, (703) 805-3918 or DSN 655-3918.

Droit et Avant!

DAVID E. QUANTOCK
Lieutenant General, USA
The Inspector General

Table of Contents

The Intelligence Oversight Guide

Introduction

Chapter 1 - Background Information

Chapter 2 - Intelligence Oversight Inspection Methodology

Appendix A - Summary of AR 381-10

Appendix B - Army G-2 Memorandum: Collecting Information on U.S. Persons

Appendix C - Sample Intelligence Oversight Inspection Directive

Appendix D - Sample Intelligence Oversight Detailed Inspection Plan

Appendix E - Sample Intelligence Oversight Unit In-Brief Presentation

Appendix F - Intelligence Oversight Training Scenario and Practical Exercises

Appendix G - Procedure 15 Reporting Format

Appendix H - Deputy Chief of Staff, G-2, Department of the Army
Intelligence Oversight Assessment / Inspection checklist

Introduction

The Intelligence Oversight Guide

1. **Purpose.** The purpose of this guide is to assist Inspectors General (IGs) in preparing, executing, and completing Intelligence Oversight inspections. The Training Division, U.S. Army Inspector General Agency, uses this guide in teaching Intelligence Oversight at the U.S. Army Inspector General School. All field IGs can use this guide in their routine Intelligence Oversight inspections.

2. **IG Responsibilities.** Every IG has a responsibility to provide Intelligence Oversight of intelligence components and activities within his or her command; inspect intelligence components as a part of the Organizational Inspection Program (OIP); and report any questionable activities in accordance with Procedure 15, AR 381-10, to HQDA (SAIG-IO). This text provides IGs with a ready reference to assist them in carrying out these responsibilities. IGs should not use this guide as a stand-alone reference during Intelligence Oversight inspections but instead should use it in conjunction with AR 381-10, U.S. Army Intelligence Activities; The Inspections Guide; and AR 1-201, Army Inspection Policy.

3. **Relationship to AR 20-1, Inspector General Activities and Procedures, and AR 1-201, Army Inspection Policy.** This guide supports the Intelligence Oversight requirements outlined in AR 20-1 and the Inspections Process described in Chapter 6 of the same document. This guide further supports the Inspection Principles and the precepts of the Organizational Inspection Program (OIP) as found in AR 1-201.

4. **Relationship to AR 381-10, U. S. Army Intelligence Activities.** This guide complements and reinforces the information found in this regulation, which is the governing document not just for the conduct of the Army intelligence activities but for Intelligence Oversight as well.

5. **Proponency**. The U.S. Army Inspector General School (TIGS) is the proponent for this guide. Please submit recommended changes or comments to the following address:

U.S. Army Inspector General School
ATTN: SAIG-TR
5500 21st Street, Suite 2305
Fort Belvoir, Virginia 22060-5935

Telephone:
Commercial: (703) 805-3900
DSN: 655-3900

TIGS relies upon the subject-matter expertise of DAIG's Intelligence Oversight Division (SAIG-IO) for the accuracy of information found in this guide. Specific questions about the conduct of Intelligence Oversight inspections and other related concerns should be directed to the Intelligence Oversight Division at the following address:

U. S. Army Inspector General Agency
ATTN: SAIG-IO
1700 Army Pentagon
Washington, DC 20310

Telephone:
Commercial: (703) 697-6698
DSN: 227-6698

6. **Format for Sample Memorandums:** This guide contains sample memorandums that do not adhere to the format requirements outlined in Army Regulation 25-50, Preparing and Managing Correspondence. In an effort to save space and paper, some of the required font sizes and spacing have been compressed. Refer to Army Regulation 25-50 for the correct format specifications.

7. **Updates.** TIGS will distribute updated versions of this guide as necessary. TIGS will notify – and then forward electronic copies to – all IG offices when changes have occurred.

8. **Summary of Change.** This revision supersedes the October 2012 version of the guide. This revision incorporates minor administrative changes throughout and the following specific changes:

a. Adds the Deputy Chief of Staff, G-2, Department of the Army Intelligence Oversight Assessment / Inspection checklist dated 19 February 2013 (Appendix H).

b. Includes several minor grammar, spelling, and doctrinal corrections (throughout).

Chapter 1

Background Information

1. **Purpose.** This chapter provides background information on Intelligence Oversight and the current rules and regulations that pertain to this system.

2. **Background Information.** During the 1960s and early 1970s, the Vietnam War strongly polarized many groups within the United States because many Americans opposed our involvement in that Southeast Asian country – often violently. These protests – and protests brought on by other issues of the 1960s such as the Civil Rights Movement – prompted many leaders at the highest levels of government to view these groups not just as political threats but also as threats to civil order. Senior leaders within the government ordered U.S. Army intelligence units and other government agencies to aggressively collect information about U.S. citizens who were involved in the anti-war and Civil Rights Movements in the belief that foreign governments were fomenting the actions of these movements.

The public soon learned about this behavior and cried foul. These intelligence-gathering activities – now deemed "Big Brother" activities – led to public demands for curbs on the intelligence community to protect against abuses of the Constitutional provision against unlawful search and seizure. President Gerald Ford responded to these public and Congressional pressures for reform with an executive order (Executive Order 11905, February 1976) that, for the first time, established rules on the collection, retention, and dissemination of information on U.S. persons. Successive presidents promulgated their own executive orders refining those rules, culminating in Executive Order 12333, which President Ronald Reagan signed during the opening weeks of his administration in 1981. Each president since President Reagan has endorsed this same executive order. The events of September 11, 2001, have not changed these rules (see Appendix B). Although the abuses that brought about the Intelligence Oversight system occurred more than 30 years ago, Intelligence Oversight requirements remain current and relevant today – especially in light of ongoing overseas contingency operations. Information operations, open-source intelligence collection, frequent deployments and stabilization operations, force protection operations, and the sharing of information between intelligence and law enforcement organizations are but a few current situations that are bringing military personnel into contact with U.S. person information and therefore demand increased Intelligence Oversight vigilance.

Many people believe that Executive Order (EO) 12333 and Army Regulation (AR) 381-10, U.S. Army Intelligence Activities, prevent military intelligence components from collecting information on U.S. Persons. This belief is false; in fact, there is no absolute ban on intelligence components collecting U.S. persons information. For all three components of the Army -- active, reserve, and National Guard -- three documents

govern such collection: EO 12333; Department of Defense Directive (DoD) 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons; and AR 381-10. Applying a three-part test can assist in determining if an intelligence component can collect information on U.S. persons:

1. Does the intelligence component have the assigned mission or function?

2. Does the information fall within one of the categories listed in DoD 5240.1-R and AR 381-10?

3. Is the least intrusive method used?

In general, collecting information on U.S. persons falls within two categories: **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 (for example, a foreign-based terrorist group). EO 12333 provides that "timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible." Don't confuse collection with receiving information that contains U.S.-persons information. Military intelligence components may receive information from anyone at anytime. If the information is U.S.-person information, military intelligence components may retain that information if it meets the three-part test discussed above. If the information received pertains solely to the functions of other Department of Defense (DoD) components or agencies outside DoD, military intelligence components may transmit or deliver that information to the appropriate recipients in accordance with Procedure 4 in AR 381-10. Remember that merely receiving information does not constitute "collection" under AR 381-10; collection entails receiving "for use." We may always receive information, if only to determine its intelligence value and whether it can be collected, retained, or disseminated in accordance with governing policy.

3. **The Intelligence Oversight System.**

a. **Standards.** EO 12333 is the current Intelligence Oversight executive order. The Department of Defense implemented and amplified that executive order in DoD Directive 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons. AR 381-10, U.S. Army Intelligence Activities, implements the DoD Directive within the Army. AR 20-1, Inspector General Activities and Procedures, specifies the role of Inspectors General in Intelligence Oversight.

b. **General.** AR 381-10 contains both broad policy guidance and very specific directions for approval of specialized investigative and collection techniques. The Army

Deputy Chief of Staff, G-2, is the policy proponent for AR 381-10. The chapters in AR 381-10 outline 15 procedures and two clarifying chapters that enable DoD intelligence components to perform effectively their authorized functions while ensuring that activities affecting U.S. persons occur in a manner that protects the Constitutional rights and privacy of such persons. All personnel assigned to, or supervising, intelligence components must, at a minimum, be familiar with Procedures 1 through 4 (General Provisions and Guidance on Collection, Retention, and Dissemination of Information on U.S. persons), Procedure 14 (Employee Conduct), and Procedure 15 (Questionable Intelligence Activities). Chapter 16 (Federal Crimes) of the regulation concerns the reporting of Federal crimes involving military intelligence (MI) personnel. Chapter 17, Support to Force Protection, Multinational Intelligence Activities, Joint Intelligence Activities, and Other Department of Defense Investigative Organizations, provides guidance for MI support of force protection programs as well as intelligence support for missions within a joint, multinational, and interagency environment. Appendix A to this guide contains summaries of the AR 381-10 chapters. With regard to Intelligence Oversight and Force Protection, IGs must note that, like Operations Security (OPSEC), force protection is a G-3 / S-3 / Provost Marshal function while an intelligence professional must perform Intelligence Oversight. The Army's Judge Advocate General (TJAG) and Army G-2 have both opined that combining into one person the roles of Intelligence Oversight Officer and the Force Protection Officer is a violation of Army policy because such a combination will likely result in a Procedure 15 violation due to the possibility of co-mingling information and databases.

c. **Applicability.** AR 381-10 applies to all Army intelligence components or activities as well as any organization, staff, or office used for foreign intelligence or counterintelligence purposes. AR 381-10 defines *intelligence activities* as all activities necessary for the conduct of foreign relations and the protection of national security pursuant to EO 12333. EO 12333 defines these activities – for the foreign intelligence and counterintelligence elements of the Army – as "military and military-related foreign intelligence and counterintelligence [gathering] . . . and information on the foreign aspects of narcotics production and trafficking." As defined by AR 381-10, *intelligence components* include the following Active Army, Army Reserve, and Army National Guard (ARNG) activities:

(1) Office of the Deputy Chief of Staff, G-2.

(2) U.S. Army Intelligence and Security Command (INSCOM) and subordinate units.

(3) 650th MI Group, Supreme Headquarters Allied Powers Europe. (This command provides National counterintelligence support to Supreme Allied Commander Europe (SACEUR) and U.S. personnel within the command).

(4) Senior intelligence officers and staffs of Army Commands (ACOMs), Army Service Component Commands (ASCCs), Direct Reporting Units (DRUs), and other commands and organizations.

(5) G-2 / S-2 offices.

(6) Installation, organization, or facility security offices when carrying out intelligence activities.

(7) Military intelligence units.

(8) U.S. Army Intelligence Center and other organizations conducting intelligence training.

(9) Intelligence systems developers when testing systems.

(10) Contractors of any Army entity when conducting intelligence activities as defined by AR 381-10.

(11) Any other Army entity when conducting intelligence activities as defined by AR 381-10.

Because military intelligence is exclusively a Federal mission, AR 381-10 controls the activities and training of the Army National Guard when using military intelligence resources and assets that the Federal government has provided, including activities or training that takes place in Title 32 status. AR 381-10 does not apply to Army intelligence components when engaged in civil disturbance or law enforcement activities. When Army intelligence activities gather information that leads to a reasonable belief that a crime has been committed, they must refer the matter to the appropriate law enforcement agency in accordance with Procedure 12 and Chapter 16 of AR 381-10. The National Guard Bureau has issued a regulation concerning Intelligence Oversight (National Guard Regulation 20-10) specifically for Army National Guard units, but this regulation must be consistent with -- and cannot supersede -- the requirements contained in AR 381-10 and AR 20-1.

d. **Responsibilities.** All personnel conducting, supervising, or providing staff oversight of intelligence activities – or are involved in any other way in intelligence activities – are charged with ensuring that those activities are conducted properly.

(1) Individuals. Each individual involved in military intelligence activities will –

- Be familiar and comply with the applicable portions of AR 381-10.

- Conduct intelligence activities strictly in accordance with U.S. law, policy, executive orders, DoD 5240.1-R, AR 381-10, and the policy of the appropriate intelligence discipline.

- Report any questionable activity in accordance with Chapter (Procedure) 15 of AR 381-10.

- Report any Federal crimes upon discovery in accordance with Chapter 16 of AR 381-10

(2) Commanders. AR 381-10 requires all commanders of units with intelligence missions to designate an intelligence professional in the intelligence operational chain to function as the organization's Intelligence Oversight Staff Officer. Commanders of units with military intelligence missions will ensure that –

- All assigned or attached personnel conducting intelligence activities do so in accordance with U.S. law, regulation, and policy.

- Military intelligence (MI) personnel and non-MI personnel conducting intelligence activities are fully aware of and comply with their individual responsibilities as outlined in AR 381-10.

- Unit personnel and supporting contractors receive the training described in paragraph 14-1 of AR 381-10 within 30 days of assignment or employment and annual refresher training as a part of the routine command-training program. Commands that have signal intelligence elements will ensure those elements obtain appropriate training from qualified personnel on applicable signal intelligence directives.

- Personnel are protected from reprisal or retaliation because they report allegations of questionable activity or Federal crimes.

- Appropriate corrective actions are imposed upon any employee who violates the provisions of AR 381-10 or policies of the appropriate intelligence discipline.

- Inspectors General; the Deputy Chief of Staff, G-2; the DoD and the Army's Office of General Counsel; and the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO) have access to all information necessary to perform their oversight responsibilities regardless of classification or compartmentation.

- Implement a review process to ensure U.S. person information was collected and retained in accordance with AR 381-10 before transferring files to the Investigative Records Repository or information into intelligence databases.

- Implement a review process to ensure U.S.-persons information incorporated into intelligence databases is maintained in accordance with the Army Records Information Management System (ARIMS).

(3) Inspectors General.

(a) AR 20-1 charges all Army IGs with providing independent oversight of intelligence components and activities within their commands. They will –

- In accordance with AR 381-10, provide Intelligence Oversight of intelligence components and activities within their command in accordance with Executive Order 12333 and DoD Directive 5240.1-R.

- Inspect intelligence activities as part of their Organizational Inspection Program.

- Report any questionable activities in accordance with Procedure 15, AR 381-10, to DAIG (SAIG-IO) within five days.

- Ensure that inspected personnel are familiar with the provisions of AR 381-10, emphasizing Chapters 1 through 4 and 14 through 17.

(b) AR 381-10 charges IGs to --

- As part of the inspection program, determine if intelligence elements are conducting foreign intelligence and counterintelligence in compliance with this and other applicable regulations.

- Ascertain whether any organization, staff, or office not specifically identified as an Army intelligence element is being used for foreign intelligence or counterintelligence purposes and, if so, ensure its activities comply with AR 381-10.

- Evaluate leadership awareness and understanding of the authorities for intelligence collection of U.S.-person information.

- Ensure that procedures exist within each element for reporting questionable intelligence activities and that personnel are aware of their reporting responsibility.

- Provide advice to the command and Intelligence Oversight Staff Officer as needed.

- Describe significant Intelligence Oversight activities and inspections and suggestions for improvement in the program for TIG's (SAIG-IO) quarterly report to the Assistant Secretary of Defense for Intelligence Oversight (ATSD-IO).

- Determine if intelligence components are involved in any questionable activity and, if such activities have been or are being undertaken, ensure the matter is investigated and corrected in accordance with paragraph 15-3, AR 381-10. If a unit involved in questionable activities did not report such matters as prescribed by AR 381-10, determine the reason for the failure and recommend appropriate corrective action.

(4) Legal Counsels. The Army's Office of General Counsel (OGC) shares responsibility for Intelligence Oversight with Army G-2 and TIG. Legal counsels at all levels provide legal interpretations of applicable law, regulations, and policies. Forward questions that cannot be resolved at the local level through command channels to Army G-2 at Headquarters, Department of the Army, for consideration by the Office of The Judge Advocate General (OTJAG). Questions that cannot be resolved at that level are referred to OGC.

(5) Army Deputy Chief of Staff (DCS) G-2. Establishes Intelligence Oversight policy within the Army and serves as the proponent for AR 381-10.

e. **Reporting.**

(1) Questionable Intelligence Activities. Procedure 15 – described in Chapter 15 of AR 381-10 – provides the process for identifying, investigating, and resolving allegations of questionable intelligence activities. Questionable activity involves conduct during or related to an intelligence activity that may violate law, Executive Order or Presidential Directive, or applicable DoD or Army policy, including AR 381-10.

(a) All Army units (active component, National Guard, and reserve) should forward all reports of questionable activity through command channels to TIG (SAIG-IO). Allegations of questionable activity must be reported in a timely manner despite the possibility that the allegation might not be substantiated. Employees have the option to report directly to the U.S. Army Inspector General Agency (SAIG-IO), the Army G-2 (DAMI-CDC), or OGC. Units must forward questionable-activity reports as soon as possible but no later than **five days** after discovery (see Appendix G for the reporting format). A reported allegation does not necessarily mean that a person or unit has violated law or policy. The fact that a questionable activity report has been submitted does not reflect negatively upon a unit; rather, it shows a unit's compliance with AR 381-10. Whenever in doubt as to whether an activity falls under Procedure 15 requirements, the unit or IG should proceed in reporting the activity for resolution at the higher levels. Regardless of which reporting channel is used, the report must reach TIG (SAIG-IO) no later than five days from discovery. TIG will provide initial and final notifications of questionable intelligence activity to the ODCS, G-2 (DAMI-CDC) and the OGC.

(b) AR 381-10 specifically charges The Inspector General (TIG) with receiving and processing all reports required under Chapter 15 and preparing and submitting a quarterly report to ATSD-IO describing significant questionable intelligence activities reported during that quarter and any resulting actions. This report includes both the active and reserve components. TIG forwards reports of questionable activity through OGC to the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO). The reporting policies directed by Procedure 15 are specifically designed to ensure that only questionable activities are reported within the Intelligence Oversight system and are in addition to command and organizational responsibilities to investigate and respond to the questionable activity in accordance with appropriate laws, policies, and

regulations. Procedure 15 provides a streamlined and expeditious reporting method to demonstrate that the Army continues to oversee the MI community and take appropriate action to correct issues. However, a Procedure 15 report is not a substitute for other required reporting requirements such as a Serious Incident Report (SIR), counterintelligence incident report, or a security violation report.

(c) Understanding the role of the National Guard Bureau (NGB) as defined in DoDD 5100.01, is essential. NGB is a joint activity of the Department of Defense, and the Chief, NGB, is a principal advisor to the Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, on matters involving non-federalized National Guard forces and other matters as determined by the Secretary of Defense. For NGB matters pertaining to the responsibilities of the Department of the Army in law or DoD policy, the Secretary of Defense normally exercises authority, direction, and control over the NGB through the Secretary of the Army. The NGB is the focal point at the strategic level for National Guard matters that are not under the authority, direction, and control of the Secretary of the Army, including joint, interagency, and intergovernmental matters where the NGB acts through other DoD officials as specified in DoDD 5105.77. This directive designates the NGB as the channel of communication on all matters pertaining to the Army National Guard and the Department of the Army and the several States. It further requires that the Chief, NGB, ensure that, in the performance of their duties, all NGB officials and personnel comply fully with applicable DoD and Department of the Army policies, issuances, publications, and legal opinions. While the Chief, NGB, may develop and promulgate directives, regulations, and publications on National Guard matters, these documents must be consistent with DoD and Department of the Army policies. National Guard Regulation (NGR) 20-10, paragraph 2-4, addresses questionable intelligence activities and requires National Guard organizations to report these activities through their chain of command to the State IG in accordance with Procedure 15 as described in DoD 5240.1-R and then to forward such reports to NGB-IGO within **five days** of discovery. This requirement is in conflict with AR 381-10, which requires that questionable intelligence activities be sent to DAIG's Intelligence Oversight Division (SAIG-IO) within five days. AR 381-10 requires the State Adjutant General to forward questionable-intelligence-activity reports to NGB, which is appropriate since NGB serves as the communications channel to the Department of the Army for matters related to the Army National Guard. In this case, AR 381-10, paragraph 15-2b, is the controlling language and requires NGB to send the questionable intelligence activity to SAIG-IO within five days of its discovery. Failing to report through SAIG-IO prevents TIG from complying with AR 381-10. Nothing in law or regulation authorizes NGB to report questionable intelligence activities directly to ATSD-IO for Army National Guard units. Please note that this guide does not address NGB processes or procedures as they relate to the Air National Guard.

(2) **Federal Crimes by Intelligence Personnel.** Chapter 16 of AR 381-10 also requires the reporting of any facts or circumstances that indicate that a member or employee of an Army intelligence component may have violated a Federal law. This chapter also applies when violations of Federal law by others comes to the attention of intelligence personnel. This Federal crime reporting is distinct from questionable-

activity reporting, and AR 381-10 provides for both of these processes. IGs do not have to become involved in Federal crime reporting unless such crimes also constitute a questionable activity. The regulation lists examples of questionable intelligence activities that constitute a crime in paragraph 15-4 and reportable Federal crimes in paragraph 16-3. Forward all reportable Federal crime reports to Army G-2 (DAMI-CDC) not later than five days after discovery or receipt at the Army Command (ACOM), Army Service Component Command (ASCC), or Direct Reporting Unit (DRU) level.

(3) **Quarterly Report of Intelligence Oversight Activities.** TIG prepares and forwards a Quarterly Report of Intelligence Oversight Activities through OGC to the ATSD-IO. The report is a compendium of questionable activity reported during the quarter, follow-up reports of ongoing investigations or inquiries regarding questionable activities, and a summary of inspections conducted by SAIG-IO during the quarter. ATSD-IO uses this report in the preparation of its own report to the President's Intelligence Oversight Board. Procedure 15, paragraph 15-6, requires specified major commands to provide input for this report to TIG but does not relieve any command or Army component (active, National Guard, or reserve) of the requirement to submit questionable intelligence activities to SAIG-IO or allow an independent submission of the Quarterly Report to ATSD-IO, which may cause duplicate reporting.

Chapter 2

Intelligence Oversight Inspection Methodology

1. **Purpose.** This chapter discusses Intelligence Oversight inspections and provides Inspectors General with a recommended methodology for conducting Intelligence Oversight inspections.

2. **Intelligence Oversight and the Organizational Inspection Program (OIP).** AR 20-1 mandates that all IGs conduct Intelligence Oversight inspections as part of their OIP, but IGs must note that the report is an IG record and that they must treat it in accordance with the rules on IG records outlined in Chapter 3 of AR 20-1. Each commander's OIP will normally determine the frequency of intelligence oversight inspections. However, IGs should inspect the intelligence components within their organizations a minimum of once every two years. IGs should orient Intelligence Oversight inspections primarily on compliance with AR 381-10, applicable Intelligence Oversight policies, applicable intelligence regulations (AR 381-20 and AR 381-12), and individual knowledge. IGs at all levels provide independent oversight of Army intelligence components within their command and should tailor their inspection to the type of unit being inspected. For example, Counterintelligence, Human Intelligence, and Signals Intelligence all have additional areas requiring inspection based on their assigned missions and authorities. The Command IG must be aware of these units and what standard(s) apply when conducting these inspections. The DAIG's Intelligence Oversight Division (SAIG-IO) inspects certain sensitive intelligence activities and a sampling of intelligence activities throughout the Army's active and reserve intelligence components.

3. **Major Tenets of an Intelligence Oversight Inspection.** An IG inspection of an intelligence component's Intelligence Oversight program is essentially a "systems check" of an existing system within that organization. Although not a systemic inspection in the purest sense, the IG must still approach the inspection with an eye toward examining that component's Intelligence Oversight program as a system within the organization but not necessarily one that has given pre-inspection indicators that the program may be suffering from a pattern of non-compliance. Instead, many IGs will conduct Intelligence Oversight inspections and find highly effective and well-managed Intelligence Oversight programs in place.

At a minimum, an Intelligence Oversight inspection should identify command intelligence components and other offices and staffs performing intelligence functions. The inspection should also determine if an Intelligence Oversight program exists and how the unit educates its personnel on applicable AR 381-10 requirements. A best practice for training, regardless of component, is to conduct initial training during unit in-processing and document it on the in-processing checklist. The inspection must identify any questionable activities; determine how violations are reported; and, if necessary, report violations found during the inspection. Again, Procedure 15 reports

must reach SAIG-IO within five days. Lastly, IG inspectors must ensure that the responsible personnel know where they can obtain expert advice. The following paragraphs describe the major parts of an Intelligence Oversight inspection.

a. **Identify command intelligence components.** Chapter 1 of this guide contains of list of the various active and reserve component activities that AR 381-10 defines as intelligence components. To identify intelligence components and personnel performing intelligence functions, ask the following questions: Where are the Military Intelligence (MI) operational units and G-2 / S-2 offices? Who (and where) are your supporting counterintelligence (CI) units? Where are the less obvious intelligence components such as security personnel, intelligence systems designers and testers, military intelligence (MI) schools, or contracted employees that perform intelligence functions?

b. **Intelligence Oversight programs.** Most intelligence components develop formal Intelligence Oversight programs and assign Intelligence Oversight responsibilities to individual units and key personnel. If a unit has such a formal program, that program should be tailored to the function and mission of the unit and the MI disciplines (such as signals intelligence) involved. Some items a local Intelligence Oversight program should address are the measures or instructions necessary to ensure U.S. person information is properly collected, retained, and disseminated; the commander's program for Intelligence Oversight training; Intelligence Oversight requirements for deployments (pre-, during, and post-deployment); Intelligence Oversight reviews for operational planning, to include any methodology to determine Intelligence Oversight risk; the availability of standardized references; the process to ensure intelligence files are reviewed annually; and the procedures for reporting questionable activities. AR 381-10 requires commanders of units with intelligence missions to designate an intelligence professional in the intelligence operational chain to function as the organization's Intelligence Oversight Staff Officer. The Intelligence Oversight program’s guidance should outline the duties and responsibilities of this officer. Soldiers and leaders within the command should know who the Intelligence Oversight officer is and the responsibilities inherent in that position. The Intelligence Oversight officer's understanding of the cooperative role shared between the IG and the Staff Judge Advocate (SJA) in the oversight of intelligence activities requires examination as well. The IG has specific oversight responsibilities as outlined in AR 20-1, and the SJA must understand AR 381-10 in order to ensure that the units stay within the boundaries of both law and policy. Note that a command Intelligence Oversight program may contain both internal and external program elements. The internal program addresses that command or headquarters while the external element concerns how a command exercises Intelligence Oversight of its subordinate commands or elements.

c. **Intelligence Oversight education.** AR 381-10, Procedure 14, paragraph 14-1, requires personnel to be familiar with AR 381-10 with an emphasis on Chapters 1 through 4 and 14 through 17. All personnel assigned to intelligence components must know that Army policy prohibits intelligence components from collecting, retaining, or

disseminating U.S. person information without the duly assigned mission or authority. All personnel must know that they should question intelligence activities that may violate law or policy and report possible violations to the chain of command or to the Inspector General. Intelligence personnel who employ specialized collection techniques need detailed knowledge on the approvals, authorities, and restrictions outlined in AR 381-10. Inspectors should check for compliance with the regulation, review training materials, and determine if personnel understand how to apply Intelligence Oversight in operational missions. See Appendix F for an Intelligence Oversight training scenario and practical exercises. The Army's Intelligence and Security Command (INSCOM) Intelligence Oversight office is an excellent source of training material and checklists for Intelligence Oversight.

d. **Identify and report questionable activities.** Determine if individuals in intelligence components know how to report a questionable activity in accordance with AR 381-10, Chapter (Procedure) 15. If you discover questionable activities during your inspection, or you are in doubt whether an intelligence component has or has not performed a questionable activity, have the intelligence component submit a Procedure 15 report as required by the regulation. DAIG's Intelligence Oversight Division (SAIG-IO) will resolve the issue with appropriate proponents and legal experts and then provide you with a response. Remember that questionable activity in the form of a Procedure 15 report must go up through command channels and reach TIG (SAIG-IO) within five days of discovery. Army National Guard units report questionable activities to their State Adjutant General, who in turn submits the report to NGB. NBG then sends a report to TIG (SAIG-IO).

4. **Sample Inspection Methodology.** The following inspection methodology (normally developed as part of the Plan-in-Detail step of the Inspections Process) is recommended for the conduct of all Intelligence Oversight inspection visits. Like all inspections, the visit should begin with an in-briefing and end with an out-briefing.

a. **In-briefing.** The inspecting IG team chief should briefly describe the conduct, techniques, and scope of the Intelligence Oversight inspection, list the inspected units, and outline to whom and when the inspection report is due. See Appendix E for an example of an IG in-briefing to the intelligence component.

b. **Inspected Unit brief.** The inspected unit should brief the IG inspection team on the unit mission, organization, operations, intelligence files, and any Intelligence Oversight policy or program. Elements of importance include the existence of an intelligence oversight program – beyond simply a written program – and a designated Intelligence Oversight Staff Officer.

c. **The IG Intelligence Oversight Inspection.**

(1) Check to ensure that the unit has a copy (or an electronic version) of AR 381-10 and any applicable changes. Also, check for any relevant Army Command (ACOM), Army Service Component Command (ASCC), Major Subordinate Command

(MSC), or unit regulations or policies that require intelligence components to maintain an Intelligence Oversight policy book. Review any policy requirements to ensure that they meet the unit's needs and the intent of the regulation. For IGs inspecting subordinate units with IGs, review the unit's OIP memorandum or regulation to ensure that the IG portion of the program includes Intelligence Oversight, and review OIP records to ensure that Intelligence Oversight inspections are occurring.

(2) Examine training records to determine whether personnel receive training on AR 381-10. Chapter (Procedure) 14 requires all personnel to receive tailored unit training within 30 days of assignment and refresher training as part of the routine command-training program. Remember that the regulation specifies that all personnel assigned to an intelligence component must be familiar with AR 381-10 and not just personnel with intelligence specialties. The regulation also requires that contractors who work on intelligence systems or conduct intelligence activities must receive Intelligence Oversight training since AR 381-10 and DoD Directive 5240.1-R consider them to be employees. The IG inspector should also review the command or unit's training package.

(3) Review the unit's OIP documents to ensure intelligence oversight is part of the command's inspection program (i.e. command inspections and staff inspections). Determine if the unit has procedures in place to follow up on deficiencies. Physically check the results of previous inspections to determine if the unit corrected problematic areas and reported and resolved matters of questionable activity in accordance with Chapter 15 (Procedure 15) of AR 381-10.

(4) As a method to determine individual knowledge, IGs can pass out copies of Intelligence Oversight training scenarios and practical exercises to intelligence-component personnel and have them brief their answers (see Appendix F). Be sure to include as many different answers as time allows. Hold discussions on why individuals answered as they did, referring to AR 381-10 and applicable Intelligence Oversight policies on each point.

(5) Review the unit procedures for handling all intelligence information (written and electronic), specifically focusing on how individuals handle U.S. person information. Determine if individuals can identify what U.S. person information is and what they would do if they came across U.S. person information. Ask how and from whom the unit receives intelligence documents, how the unit analyzes this information and produces its own intelligence products, and how and to whom the unit disseminates the products.

(6) Physically check the intelligence files for U.S. person information. Look at both paper and electronic files. Concentrate on threat files, particularly Force Protection files, Operational Plans (OPLANs), and Intelligence Summaries (INTSUMs). Crosswalk unit intelligence files with disciplinary and derogatory files involving intelligence personnel to determine whether a relationship to questionable activity existed and whether the unit complied with the provisions of AR 381-10. Also, check to

see whether the organization or activity has documented an annual review of its files for U.S.-person information.

(a) Unauthorized collection by corps and division intelligence components often occurs when Force Protection or antiterrorism information is incorrectly included in the intelligence products. Military Intelligence units may be trying to do the Provost Marshal's job. Unless authorized under Chapter 12 (Procedure 12) of AR 381-10, military intelligence components do not have a mission to retain information on U.S. domestic threats; those threats are a law enforcement and Provost Marshal function. The G-2 / S-2 is not involved in antiterrorism on the domestic front, which is an operations function as outlined in AR 525-13. This delineation of responsibility does not mean that Military Intelligence components should not pass information of this type to the appropriate authorities; the key point is that intelligence components should not collect, retain, and disseminate this kind of information for Military Intelligence purposes.

(b) There may be circumstances where the retention of an intelligence file with U.S. person information is appropriate. For instance, the Military Intelligence component may keep Information about a "non-targeted" U.S. person acquired incidentally to an otherwise authorized collection as long as the information meets the retention criteria of Chapter 3 (Procedure 3) of AR 381-10. Also, Military Intelligence components may temporarily retain U.S. person information for up to 90 days solely to determine if the information is, in fact, retainable under AR 381-10. The 90-day period starts upon the unit's receipt of the information.

(c) Personnel security information is NOT Military Intelligence information. This information is considered administrative in nature by AR 381-10 and is governed by AR 380-67. Unit S-2s and garrison intelligence and security divisions are authorized to retain information necessary to support the processing of security clearances.

(7) Check for an annual review of intelligence files and databases. AR 381-10, Chapter 3 (Procedure 3), directs intelligence components to review intelligence files and databases annually. The review – which the unit can conduct incrementally as long as all holdings are reviewed annually – ensures that any retention of U.S. person information is only for authorized functions, is not held beyond the established disposition criteria, and is not retained in violation AR 381-10. These reviews should normally be conducted in concert with a review of files required by AR 25-400-2, The Army Records Information Management System (ARIMS). The unit should maintain a record of these reviews and identify the specific U.S.-person information they must retain for approved mission purposes.

(8) Military Intelligence support to Civilian Law Enforcement Authorities (CLEA) (Procedure 12). Pay particular attention to files relating to support given to civilian law enforcement and to domestic-threat assessments for Continental United States (CONUS) military installations. Except for emergencies, approval for support to CLEA and the Federal Bureau of Investigation must come from the Secretary of Defense.

Units that have provided support to civilian law enforcement agencies are particularly vulnerable to violations of AR 381-10 – especially when after-action reports and threat assessments are brought back from the support missions and incorporated into U.S. Army intelligence files. When the intelligence personnel are on authorized missions supporting a civilian law enforcement agency, they may collect certain information on U.S. persons. That information, however, remains the property of the law enforcement agency, and the intelligence component may not retain this information in intelligence files. Individuals with a military intelligence Military Occupational Specialty (MOS) may be detailed to support law enforcement efforts based upon their specific skills, but their activities should not be co-mingled with work in their military intelligence field or create the perception that a U.S. Army Military Intelligence component is collecting U.S. person information.

(9) Finally, determine if the intelligence component knows how to report a questionable activity in accordance with AR 381-10, Chapter (Procedure) 15, and reportable Federal crimes under Chapter 16. Does an Intelligence Oversight point of contact (POC) exist for the command or in the intelligence component? Do unit members know who the Intelligence Oversight POC is and the role of the Intelligence Oversight Staff Officer? Do they understand the IG role in Intelligence Oversight? Is the command's Staff Judge Advocate (SJA) knowledgeable regarding Intelligence Oversight and the reporting of questionable activities and Federal crimes? If the intelligence component discovers or suspects questionable activities, the unit must submit a Procedure 15 report immediately.

d. **Out-briefing.** Discuss any possible Intelligence Oversight issues identified during the inspection with the intelligence component's leadership. Inform the unit that these issues are just issues and not findings or observations until you can crosswalk (or verify) them.

5. **DAIG Tip**: The underlying principle for Intelligence Oversight is to ensure that any Army component performing authorized intelligence functions carries out those functions in a manner that protects the Constitutional rights of U.S. Persons. The rules for Intelligence Oversight apply throughout the Army: the Army may only maintain personal information that is necessary to accomplish a purpose or mission of the Army as required by Federal statute or executive order (also see AR 340-21, The Army Privacy Program, paragraph 4-1). AR 381-10 simply provides for additional oversight as well as procedures that allow intelligence components to handle U.S.-person information when it is necessary to accomplish the intelligence mission. When IGs encounter U.S.-person information in the files of an intelligence component, the three primary questions the component must answer are as follows: (1) *What is your mission?,* (2) *What is your authority?*, and (3) *Is this the least intrusive method?* Issues that arise during an Intelligence Oversight inspection usually involve individuals trying to do the right thing but not understanding the correct authority that governs their mission or the failure to obtain the correct approval for Procedures 5 to 13.

Appendix A

Summary of AR 381-10

1. **Purpose.** This appendix provides a summary of the 17 Intelligence Oversight chapters outlined in AR 381-10.

2. **Chapter 1 (Procedure 1) – General Provisions.** Chapter 1 describes the purpose, responsibilities, and the applicability of the regulation and the general principles governing intelligence activities.

a. Department of the Army (DA) intelligence components must*:*

(1) Not infringe upon the Constitutional rights of any United States (U.S.) person;

(2) Protect the privacy rights of all persons entitled to such protection;

(3) Be based on a lawfully assigned function;

(4) Employ the least intrusive, lawful techniques; and

(5) Comply with all regulatory requirements.

b. AR 381-10 does not in itself authorize intelligence activity. The Army element must first have the mission and authority to conduct the intelligence activity and, when duly authorized, must comply with the provisions of AR 381-10. In addition, the fact that a collection category exists does not convey authorization to collect. There must be a link between the U.S. person information and the element's assigned mission and function, to include the exploitation of open-source data.

c. Participation of military intelligence components in special activities (see definition of special activities in Glossary of AR 381-10) is prohibited unless the President, Secretary of Defense, and Service Secretary have approved the special activity. Assassinations are specifically forbidden for military intelligence (MI) personnel as is requesting any other party to perform an activity that MI personnel are prohibited from performing.

d. AR 381-10 does not apply to law enforcement activities, including civil disturbance operations. Procedure 12 requires Secretary of Defense concurrence for support to civilian law enforcement authorities by intelligence components. When intelligence components collect information that provides a reasonable belief that a crime has been committed, they are obligated to report that information to the appropriate law-enforcement agency in accordance with Procedure 12 and Chapter 16.

e. A person or organization outside the U.S. – or an alien within the United States – is presumed **not** to be a U.S. person unless the intelligence component obtains specific information to the contrary.

3. **Chapter 2 (Procedure 2) - Collecting U.S. Persons Information.**

a. This chapter specifies the kinds of U.S. person information that MI components may collect and the general means by which information may be collected. The core tenet of AR 381-10 is that MI components may collect U.S. person information only when necessary to fulfill an assigned function and the collection activity falls into one of 13 categories listed in Procedure 2.

b. The definition of collected can cause confusion. AR 381-10, Glossary, defines collection as follows:

Information is *collected* when an intelligence employee gathers and receives the information in the course of official duties and the employee intends to use the information for intelligence purposes. An employee must take an action that demonstrates intent to use or retain the information, such as producing an intelligence information or incident report or adding the information to an intelligence database. Data acquired by electronic means (for example, telemetry, signals traffic analysis, and measurement and signatures intelligence) is “collected” only when it has been processed from digital electrons into a form intelligible to a human being. Information held or forwarded to a supervisory authority solely for a collectability determination, and not otherwise disseminated within the intelligence component, is not “collected.”

c. A U.S. Person is any entity meeting one of the following criteria:

(1) A U.S. citizen,

(2) An alien known by the intelligence component to be a permanent resident alien,

(3) An unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or

(4) A corporation incorporated in the United States that is not directed or controlled by a foreign government.

d. When authorized, MI components may collect U.S. person information by any lawful means but must exhaust the least intrusive collection means before requesting a more intrusive method. The least intrusive means would involve using publicly available sources or information with the U.S. person's consent. Only when information cannot be gained from open sources, or with the consent of the U.S. person, will more intrusive means be used to the extent of the law. Within the United States, only overt means

may be used to collect foreign intelligence information on U.S. persons unless stringent tests are met as specified in paragraph 2-4, Chapter (Procedure) 2 e. Absolutely nothing in Procedure 2 can be interpreted as an authority to collect information relating to a U.S. person solely because of that person's lawful -- and constitutionally protected -- advocacy of measures opposed to Government policy.

4. **Chapter 3 (Procedure 3) - Retaining U.S. Person Information.**

a. Information is defined as *retained* only if it can be retrieved by the person's name or other personal identifying data.

b. Retention of U.S. person information is authorized under the following criteria:

(1) The Information was properly collected under Procedure 2.

(2) The information was acquired incidentally to an otherwise authorized collection and such information –

(a) Could have been collected under Procedure 2,

(b) Is necessary to understand or assess foreign intelligence or counterintelligence,

(c) Is foreign intelligence or counterintelligence collected from authorized electronic surveillance, or

(d) Is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.

c. Access to U.S.-person information will be restricted to certain individuals on a need-to-know basis. Intelligence components will review their intelligence files annually. This review will specifically focus on U.S. person information to determine whether continued retention serves the purpose for which it was retained and that continued retention is necessary to an assigned function.

5. **Chapter 4 (Procedure 4) - Dissemination of Information about U.S. Persons.**

a. This chapter governs the types of information regarding U.S. persons that may be disseminated – without the person's consent – outside of the Army intelligence component which collected and retained the information. This procedure does not apply to information collected solely for administrative purposes or disseminated pursuant to law or proper court authority.

b. Non-signals intelligence information about a U.S. person may be disseminated without that person's consent under the following conditions: (1) The information was

collected or retained under the provisions of Procedures 2 and 3; or (2) The recipient is reasonably believed to have a need for the information to fulfill a lawful assigned governmental function and that recipient is a member of one of the agencies listed in paragraph 4-2 of Chapter (Procedure) 4.

6. **Chapters (Procedures) 5 through 10** deal with limitations on -- and approval procedures for -- specialized collection techniques. The specific techniques covered are electronic surveillance, concealed monitoring, physical searches, searches and examination of mail, physical surveillance, and undisclosed participation in organizations.

7. **Chapter 11 (Procedure 11) - Contracting for Goods and Services.**

a. MI elements can enter into contracts with academic institutions only if an intelligence component informs the appropriate officials of that sponsorship.

b. MI elements may contract with commercial organizations, private institutions, or individuals within the U.S. without revealing their intelligence affiliation only if:

(1) The contract is for published material available to the general public or for routine goods and services necessary for the support of approved activities, or

(2) The Secretary or Under Secretary of the Army makes a written determination that sponsorship must be concealed to protect an intelligence activity.

8. **Chapter 12 (Procedure 12) - Assistance to Civilian Law Enforcement Authorities.**

a. Upon approval of the Secretary of Defense, MI components may assist Civilian Law Enforcement Authorities (CLEA) for the following purposes:

(1) Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities.

(2) Protecting DoD employees, information, property, facilities, and information systems.

(3) Preventing, detecting, or investigating other violations of law.

b. MI components may assist civilian and military law enforcement with the following activities:

(1) Disseminating incidentally acquired information believed to indicate a violation of Federal, state, or foreign law.

(2) Providing specialized equipment and facilities to Federal authorities and, when lives are endangered, to state and local authorities in accordance with DoD Directive 5525.5.

(3) Providing intelligence personnel to Federal authorities and, when lives are endangered, to state and local authorities in accordance with DoD Directive 5525.5 and Army General Counsel concurrence.

(4) Providing assistance to foreign government or foreign law enforcement and security services in accordance with theater policy and applicable Status of Forces Agreements (SOFA).

9. **Chapter 13 (Procedure 13) - Experimentation on Human Subjects for Intelligence Purposes.**

MI experimentation with human subjects may only be performed with the consent of the subject in accordance with established medical guidelines and with the approval of the Secretary of the Army, Under Secretary of the Army, Secretary of Defense, or Deputy Secretary of Defense as appropriate.

10. **Chapter 14 (Procedure 14) - Employee Conduct.**

a. Training. All personnel conducting, supervising, or providing staff oversight of intelligence activities will be familiar with AR 381-10 with emphasis on Chapters 1 through 4 and 14 through 17. Those employees involved in the activities described in Chapters 5 through 13 will be familiar with the provisions of those procedures as well.

(1) MI employees must receive tailored training within 30 days of assignment or employment and refresher training as part of the routine command training program.

(2) Commands that have signal intelligence cryptologic elements must obtain appropriate training from qualified personnel on applicable Signal Intelligence directives.

b. Individual Responsibilities. All employees will –

(1) Conduct intelligence activities in accordance with applicable law and policy, AR 381-10, and the policy of the appropriate intelligence discipline.

(2) Familiarize themselves with this regulation and applicable Signal Intelligence directives.

(3) Report questionable intelligence activities and Federal crimes in accordance with Chapters 15 and 16.

c. Command Responsibilities. Commanders will ensure –

(1) Personnel are protected from reprisal and retaliation because they report allegations in Chapters 15 and 16.

(2) Appropriate sanctions are imposed upon any employee who violates the provisions of this regulation and Signal Intelligence directives.

(3) The field IG; the DCS, G-2; TIG; the Army General Counsel; and the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO) have access to information necessary to perform their oversight responsibilities regardless of classification or compartmentation.

(4) Employees cooperate fully with the President's Intelligence Oversight Board.

(5) All proposals for intelligence activities that may be unlawful – in whole or in part – or may be contrary to policy will be referred to the Army General Counsel.

11. **Chapter 15 (Procedure 15) - Questionable Intelligence Activities.**

a. All U.S. Army employees and supervisors in all Army components will report questionable intelligence activities upon discovery through command or inspector general channels to DAIG's Intelligence Oversight Division (SAIG-IO) with an information copy to the DCS, G-2 (DAMI-CDC) within five days from discovery. Reports may be made by e-mail, facsimile, message, or hard copy; the reports may be classified at any level, to include special-access program caveats as necessary. Questionable intelligence activities include suspected misconduct in the performance of any intelligence activity or mission.

b. The reporting command will submit status reports on the questionable activity every 30 days to SAIG-IO until they complete the investigation. Status reports are not required when the allegation is referred for a counterintelligence or criminal investigation until the investigation is complete.

c. A command may choose to conduct an inquiry of the questionable activity under the provisions of AR 15-6 or through the appropriate IG; however, this inquiry does not alleviate or satisfy the initial five-day reporting requirement to SAIG-IO. All reports must receive a legal review to confirm or refute the allegation and assess whether the reported activity is consistent with applicable policy. Other than counterintelligence or criminal investigations, commands will complete the inquiries within 60 days of the initial report and inform SAIG-IO of the inquiry's results.

d. As part of their oversight inspections, IGs will seek to determine if intelligence components are involved in questionable activities and, if so, report such activities under Procedure 15.

12. **Chapter 16 – Federal Crimes.**

a. Reports of Federal crimes involving MI personnel must be forwarded through command channels to the DCS, G-2 (DAMI-CDC); the Provost Marshal General; and the U.S. Army Criminal Investigations Command. These reports will reach DCS, G-2, within five days after discovery or receipt at the Army Command (ACOM), Army Service Component Command (ASCC), or Direct Reporting Unit (DRU) level.

b. Federal crimes that are also questionable intelligence activities will be reported as a Procedure 15 report with an explanation of why the activity meets both criteria. If the unit initially reported the Federal crime under AR 190-40, the Serious Incident Report (SIR) date-time group will be provided or a copy attached.

13. **Chapter 17 – Support to Force Protection, Multinational Intelligence Activities, Joint Intelligence Activities, and Other Department of Defense Investigative Organizations.**

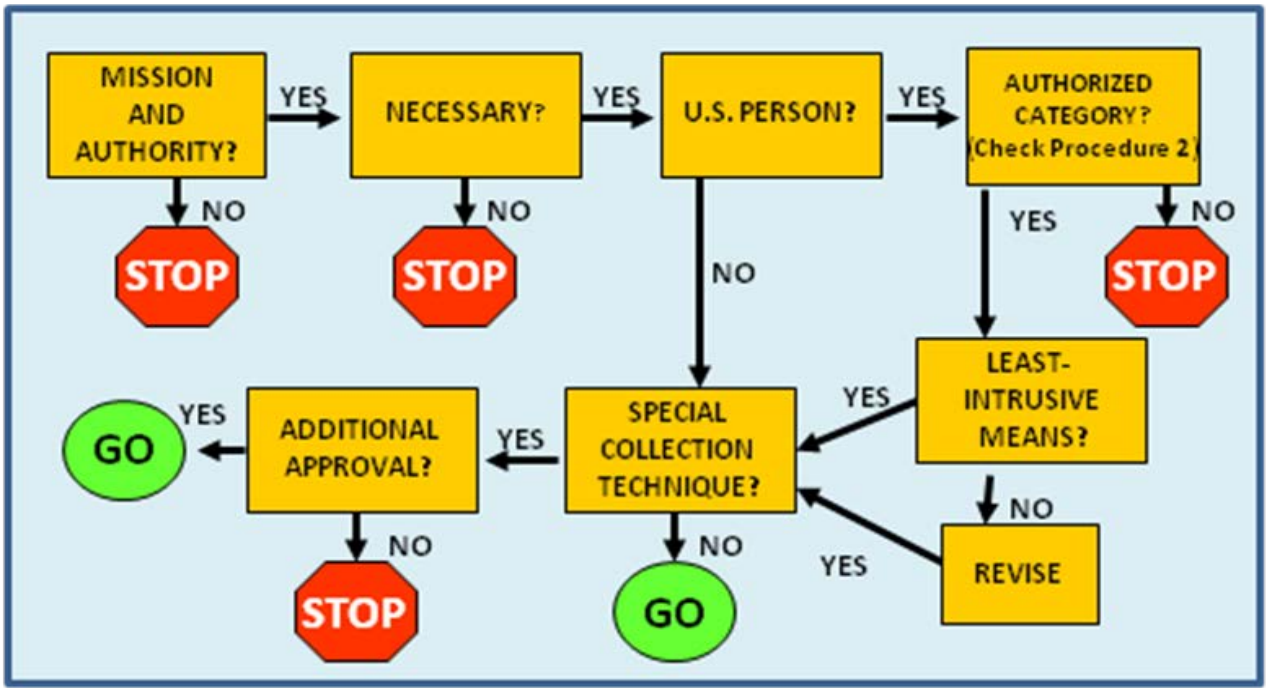
a. MI support to force protection is limited to identifying, reporting, analyzing, and disseminating intelligence regarding *foreign* threats in the Army. Civilian Federal, State, and local law enforcement authorities have the primary responsibility for information collection to protect U.S. military forces within the United States. Special agents from the U.S. Army Criminal Investigations Command (USACIDC) serve as the Army's primary liaison and representative to U.S. civilian law enforcement authorities (CLEA) for exchanging criminal intelligence, and the Army counterintelligence personnel serve as the primary liaison representative to U.S. CLEA for exchanging foreign threat information.

b. Within multinational commands, U.S. intelligence personnel may not participate in activities prohibited by law, policy, or regulation. Also, a U.S. Army commander of a multinational unit may not direct non-U.S. personnel to conduct activities that are prohibited by U.S. law, policy, or regulation. A U.S. judge advocate with intelligence law experience or training must review multinational intelligence activities for U.S. legal sufficiency.

c. Army personnel assigned to a joint command must be familiar with the policies of DoD and other military intelligence organizations. Army MI components will comply with their own service component policies unless otherwise specified in writing by the joint force commander.

d. Army counterintelligence (CI) may cooperate with DoD investigative organizations (i.e., USACIDC) for CI functions, criminal cases involving classified defense information, or other investigations in which these law enforcement elements have the lead.

14. **AR 381-10 Flow Chart.** The following flow graphically portrays the general process for determining an intelligence component's collection and other authorities outlined in detail in AR 381-10.



Appendix B

Army G-2 Memorandum: Collecting Information on U.S. Persons

1. **Purpose.** This appendix provides a precise copy of the Army G-2's (then the Deputy Chief of Staff for Intelligence, or DCSINT) memorandum on Collecting Information on U.S. Persons (dated 5 November 2001).

2. **Specific Text.** The specific text of the memorandum is as follows:

DAMI-CDC (25-30q) 05 Nov 01

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Collecting Information on U.S. Persons

1. The 11 September 2001 terrorist attack on America presented the United States and the U.S. Army with unprecedented challenges. Both our nation and our Army are responding vigorously to these challenges and will ultimately be victorious over international terrorism. Achieving this victory will not be easy, however. Our adversary is not a clearly defined nation state with fixed borders or a standing army. It is, instead, a shadowy underworld operating globally with supporters and allies in many countries, including, unfortunately, our own. Rooting out and eliminating this threat to our freedom and way of life will call upon every resource at our disposal. I am proud to say that Army Military Intelligence (MI) will play a pivotal role in helping to defeat this threat.

2. Many of the perpetrators of these attacks lived for some time in the United States. There is evidence that some of their accomplices and supporters may have been U.S. persons, as that term is defined in Executive Order (EO) 12333. This has caused concern in the field regarding MI's collection authority. With that in mind, I offer the following guidance:

a. Contrary to popular belief, there is no absolute ban on intelligence components collecting U.S. person information. That collection, rather, is regulated by EO12333 and implementing policy in DoD 5240.1-R and AR 381-10.

b. 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 AR 381-10. The two most important categories for present purposes 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).

3. EO 12333 provides that "timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible." That said, my staff has received reports from the field of well-intentioned MI personnel declining to receive reports from local law enforcement authorities, solely because the reports contain U.S. person information. 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 discussed in paragraph 2b, above. 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 Procedure 4, AR 381-10. Remember, merely receiving information does not constitute "collection" under AR 381-10; collection entails receiving "for use." Army intelligence may always receive information, if only to determine its intelligence value and whether it can be collected, retained, or disseminated in accordance with governing policy.

4. Military Intelligence must collect all available information regarding international terrorists who threaten the United States and its interest, including those responsible for planning, authorizing, committing, or aiding the terrorist attacks of 11 September 2001. We will do so – as EO 12333 directs – "in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law, and respectful of the principals upon which the United States was founded."

5. Key ODCSINT numbers for intelligence oversight questions are (703) 601-1958 / 1551, or through the 24-hour Intelligence Watch at (703) 697-5484 / 5485.

ROBERT W. NOONAN, JR.
Lieutenant General, GS
Deputy Chief of Staff
For Intelligence

DISTRIBUTION:
DAMI
MACOMs
USAICFH

CF:
ATSD(IO), SAIG-IO
SAGC, DAJA-IO

Appendix C

Sample Intelligence Oversight Inspection Directive

DEPARTMENT OF THE ARMY
HEADQUARTERS, 66th INFANTRY DIVISION
FORT VON STEUBEN, VIRGINIA 12345

AFVS 14 April ____

MEMORANDUM FOR THE INSPECTOR GENERAL

SUBJECT: Directive for Inspection (Intelligence Oversight Program)

1. You are directed to evaluate the compliance of the 66th Infantry Division's Intelligence Oversight Program with an emphasis on integration of Intelligence Oversight in daily operations.

2. The assessment will focus on the following objectives:

a. Determine if military intelligence components within the Division are complying with the provisions of AR 381-10.

b. Determine if military intelligence (MI) components are effectively training all assigned, attached, and contracted MI personnel on intelligence oversight.

c. Determine if intelligence oversight is integrated into the unit's Organizational Inspection Programs (OIP).

d. Determine if questionable activities or Federal crimes committed by intelligence personnel are reported and resolved in accordance to AR 381-10.

3. You are authorized to task the Division staff and subordinate headquarters for those resources required to ensure the successful accomplishment of this assessment.

4. Within the limits of your security clearances, you are authorized unlimited access to Division activities, organizations, and all information sources necessary to perform your oversight duties, regardless of compartmentation.

5. You will provide me with a mid-course progress review at the end of July followed by a written report not later than 1 September.

6. Upon discovery, you will notify me of any questionable activity or Federal crimes found during the inspection.

MOTTIN De La BLAME
Major General, USA
Commanding

Appendix D

Sample Intelligence Oversight Detailed Inspection Plan

DEPARTMENT OF THE ARMY
HEADQUARTERS, 66TH INFANTRY DIVISION
FORT VON STEUBEN, VIRGINIA 12345

AFVS-IG 2 May ____

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Detailed Inspection Plan for the Intelligence Oversight Inspections

1. DIRECTIVE: On 14 April ____, the Commanding General (CG) directed the Inspector General to conduct General Inspections of the Intelligence Oversight Programs within the 66th Infantry Division. Unlike most Inspector General (IG) inspection reports, the IG will not redact unit names from the final written report to the CG because this inspection will be a general inspection to determine if intelligence components are in compliance with Intelligence Oversight policies.

2. INSPECTION PURPOSE: The purpose of these inspections is to evaluate the compliance of the 66th Infantry Division's Intelligence Oversight Programs with an emphasis on integration of Intelligence Oversight in daily operations.

3. OBJECTIVES: The objectives for these inspections are as follows:

a. Determine if military intelligence components within the Division are complying with the provisions of AR 381-10.

b. Determine if military intelligence (MI) components are effectively training all assigned, attached, and contracted MI personnel on intelligence oversight.

c. Determine if intelligence oversight is integrated into the unit's Organizational Inspection Programs (OIP).

d. Determine if questionable activities or Federal crimes committed by intelligence personnel are reported and resolved in accordance to AR 381-10.

4. TASK ORGANIZATION: An inspection team from the Inspections Branch of the 66th Infantry Division Inspector General Office will conduct the inspections by inspecting five active-duty divisional units. The composition of the team and each person's security clearance is as follows:

MAJ List (Team Leader) – Top Secret
CPT Numero (Deputy Team Leader) –Top Secret
MSG Smith (Team NCOIC) – Top Secret
SFC Bergerac – Secret
CW3 Cloak (MI augmentee) – Top Secret
MSG Dagger (MI augmentee) – Top Secret

5. INSPECTED UNITS: The inspection will involve the following units and staff agencies on the dates indicated:

20 July: Company B (MI), 2nd STB
22 July: Company B (MI), 3rd STB
26 July: Company B (MI), 1st STB
30 July: Division G-2 and ACE
1 August: Company B (MI), 4th STB

6. INSPECTION APPROACH: The inspection team will spend one day inspecting each unit. The respective unit will draft an itinerary for the Inspection Team based upon guidance outlined in paragraph nine of this document. The basic inspection approach at each location will be to in-brief the unit leaders and staff members; receive a briefing from the inspected unit on Intelligence Oversight compliance efforts; review relevant documents related to Intelligence Oversight; survey Commanders, Intelligence Oversight Staff Officer or points of contact (POCs), junior officers, NCOs, and Soldiers through interviews and sensing sessions; and physically check paper and electronic intelligence files for U.S. person information.

a. Personnel to Interview (see paragraph seven below for specific requirements):

- Company Commander / XO / 1SG / Intelligence Oversight Staff Officer or POC
- Junior Officers / Warrant Officers
- NCOs (E-5 to E-7)
- Soldiers

b. Documents to Review:

- Division, Brigade, Battalion, Company Intelligence Oversight Program documents
- Results of any command or staff inspections of Intelligence Oversight
- Results of annual review of intelligence files and databases

- Intelligence files (paper and electronic)
- Records of intelligence oversight training
- Records of any previous Procedure 15 reports and investigations

7. INTERVIEW REQUIREMENTS:

a. The following table outlines the specific interview and sensing-session requirements for a standard MI company:

	Commander	**1SG**	**XO**	**IO Staff Officer / POC**	**Junior Officers**	**NCOs**	**Soldiers**
Individual Interviews	1	1	1	1			
Sensing Session: Junior Officers / Warrant Officers					8		
Sensing Session: NCOs						8	
Sensing Session Soldiers							12
Total Contacted	**1**	**1**	**1**	**1**	**8**	**8**	**12**

b. Classroom and Interview Location Requirements. Each sensing session will require a classroom or similar facility that is removed from the unit's normal work location. The area must be relatively quiet and free from interruptions and telephone calls. In addition, the room will need no fewer than eight chairs or desks formed in a circle or "U" shape. The unit should schedule 90-minute blocks for each sensing session. Individual interviews can occur in the interviewee's office or in a similar location that is free from interruptions and telephone calls. The unit should schedule these interviews to last no more than one hour.

8. SPECIAL AREA OF INTEREST. The Inspection Team will not address a Special-Interest Item (SII) during this inspection.

9. INSPECTION ITINERARIES: The Inspection Team requests a draft itinerary that meets the requirements listed in paragraphs six and seven no less than 10 days before the day of the scheduled inspection. These itineraries should go directly to the Team

Leader (see paragraph four). The Team Leader will work with each unit to determine which itinerary best allows the Inspection Team to meet the objectives listed in paragraph three. The intent of each inspection team is to conduct this assessment with minimal disruption to ongoing training. The team requires no special calendar arrangements except for the scheduling of group sensing sessions, interviews, and in- and out-briefings. A sample itinerary for a one-day unit inspection is as follows:

0800-0815	In-Brief Commander and Unit Leaders
0815-0900	Inspected Unit Brief
0900-1000	Interview Commander
0900-1030	Sensing Session with Junior Officers and Warrant Officers
0900-1200	Review Documents
1000-1100	Interview First Sergeant
1030-1200	Sensing Session with NCOs
1100-1200	Interview Executive Officer
1300-1400	Interview Intelligence Oversight Staff Officer or Point of Contact
1300-1430	Sensing Session with Soldiers
1300-1530	Review Intelligence Files
1530-1630	Inspection Team In-Process Review (IPR)
1645-1715	Out-Brief Commander and Unit Leaders

10. PRE-INSPECTION DOCUMENT REQUEST: The Inspection Team requests that each unit send the following documents -- as they apply -- to the inspection Team Leader:

- Division, Brigade, Battalion, and Company Intelligence Oversight Program documents
- Results of any command or staff inspections of Intelligence Oversight
- Results of annual review of intelligence files and databases
- Records of any previous Procedure 15 reports and investigations

The intent of this document request is to view only those documents that relate to Intelligence Oversight. Avoid sending documentation that does not apply to Intelligence Oversight. These documents are due to the Inspection Team Leader not later than 10 days before the scheduled inspection. Electronic versions of these documents sent via email are acceptable. Contact the Team Leader if any of the pre-inspection documents requested by the IG contain classified or compartmented information.

11. RESOURCES: The Inspection Team will travel to each unit using a locally procured TMP van. The team members do not require any additional transportation. The unit will provide other special equipment to the team members as required.

12. ADMINISTRATIVE SUPPORT REQUIREMENTS: The Inspection Team will require the following administrative support assistance from each unit:

a. Desk space for three or more people

b. Access to a computer

c. Printer and copying support

13. REPORT COMPLETION TIMELINE: The results of each intelligence component's inspection will be contained in a written report provided to the Division Commander. The schedule to complete the report is as follows:

a. Out-brief the Commanding General: 14 August ____

b. Complete report: 1 September ____

14. SUSPENSE SUMMARY: A summary of the suspenses contained in this document is as follows:

a. Draft itineraries due to the Inspection Team no less than **10 days** before the date of the scheduled inspection.

b. Requested documents due to the Inspection Team no less than **10 days** before the day of the scheduled inspection.

15. POC for this inspection is MAJ List, (703) 123-5678 or DSN: 555-5678, frank.list@ignet.army.mil.

Encl
Inspection Directive

ALBERT R. RIGHTWAY
LTC, IG
Inspector General

DISTRIBUTION:
G-2
Commander, 1st BCT
Commander, 2nd BCT
Commander, 3rd BCT
Commander, 4th BCT
Commander, 1st STB
Commander, 2nd STB
Commander, 3rd STB
Commander, 4th STB

CF:
SJA

Appendix E

Sample Intelligence Oversight Unit In-Brief Presentation

INTELLIGENCE OVERSIGHT INSPECTION

General Inspection of the
Intelligence Oversight Program

Inspection In-Briefing
Company B (MI)
1st Special Troops Battalion (STB)
20 July _____

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Inspection Purpose

The purpose of these inspections is to evaluate the compliance of the 66th Infantry Division's Intelligence Oversight Programs with an emphasis on integration of Intelligence Oversight in daily operations.

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Inspection Objectives

1. Determine if military intelligence components within the Division are complying with the provisions of AR 381-10.
2. Determine if military intelligence (MI) components are effectively training all assigned, attached, and contracted MI personnel on intelligence oversight.
3. Determine if intelligence oversight is integrated into the unit's Organizational Inspection Programs (OIP).
4. Determine if questionable activities or Federal crimes committed by intelligence personnel are reported and resolved in accordance to AR 381-10.

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

IG Ground Rules

- Always on the record
- Can look into any violation of law or regulation
- Available for IG assistance
- Here to help; our goal is to --
  - Be value added
  - Identify issues affecting mission / operations
  - Identify systemic issues

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

IG Reporting

- Unlike most Inspector General (IG) inspection reports, we will attribute our findings to specific units in the final written report to the Commanding General.
- We will not release the final written report to anyone beyond the CG unless directed by The Inspector General of the Army.
- We will report the discovery of questionable activities or Federal crimes in accordance with AR 381-10.

INTELLIGENCE OVERSIGHT INSPECTION

IG Task Organization

- MAJ List (Team Leader) – Top Secret
- CPT Numero (Deputy Team Leader) –Top Secret
- MSG Smith (Team NCOIC) – Top Secret
- SFC Bergerac – Secret
- CW3 Cloak (MI augmentee) – Top Secret
- MSG Dagger (MI augmentee) – Top Secret

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Inspection Methodology

The basic approach for today's inspection will be to –

- ❑ Receive a briefing from the inspected unit on Intelligence Oversight compliance efforts
- ❑ Review relevant documents related to Intelligence Oversight
- ❑ Survey Commanders, Intelligence Oversight Staff Officers or Points of Contact (POC), junior officers, NCOs, and Soldiers through interviews and sensing sessions
- ❑ Physically check paper and electronic intelligence files for U.S. person information

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Personnel to Interview

Individual Interviews (POC is MAJ List):

- – Company Commander
- – First Sergeant
- – Executive Officer
- – Intelligence Oversight Staff Officer or POC

Sensing Sessions (POC is MSG Smith):

- – Junior Officers / Warrant Officers
- – NCOs (E-5 to E-7)
- – Soldiers

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Documents to Review

(POC is CW3 Cloak and MSG Dagger)

- Division, Brigade, Battalion, and Company Intelligence Oversight Program documents
- Results of any command or staff inspections of Intelligence Oversight
- Results of annual review of intelligence files and databases
- Records of intelligence oversight training
- Records of any previous Procedure 15 reports and investigations
- Intelligence files (paper and electronic)

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Inspection Itinerary

0800-0815	In-Brief Commander and Unit Leaders
0815-0900	Inspected Unit Brief
0900-1000	Interview Commander
0900-1030	Sensing Session with Junior Officers and Warrant Officers
0900-1200	Review Documents
1000-1100	Interview First Sergeant
1030-1200	Sensing Session with NCOs
1100-1200	Interview Executive Officer
1300-1400	Interview Intelligence Oversight Staff Officer or Point of Contact
1300-1430	Sensing Session with Soldiers
1300-1530	Review Intelligence Files
1530-1630	Inspection Team In-Process Review (IPR)
1645-1715	Out-Brief Commander and Unit Leaders

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Questions?

Intelligence Oversight Points of Contact

- IG, LTC Rightway, (703) 123-5677 or DSN: 555-5677, wally.rightway@ignet.army.mil
- IG Inspections Chief, MAJ List, (703) 123-5678 or DSN: 555-5678, frank.list@ignet.army.mil
- IG Inspections NCOIC, MSG Smith, (703) 123-5678 or DSN: 555-5678, john.smith@ignet.army.mil
- Staff Judge Advocate, COL Beagle, (703) 123-3401 or DSN: 555-3401

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Back-Up Slides

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Intelligence Oversight (AR 381-10)

- **Implements Executive Order (EO 12333)**
- **Provides procedures on:**
  - **Collection, dissemination, or retention of information on U.S. persons by intelligence components.**
  - **Use of intrusive collection techniques (surveillance, bugging, phone taps).**
  - **Assistance by intelligence components to law enforcement.**
  - **Employee Misconduct. Reporting violations, investigating, and taking corrective action.**

INTELLIGENCE OVERSIGHT INSPECTION

Command Intelligence Oversight Requirements

In accordance with AR 20-1 and AR 381-10:

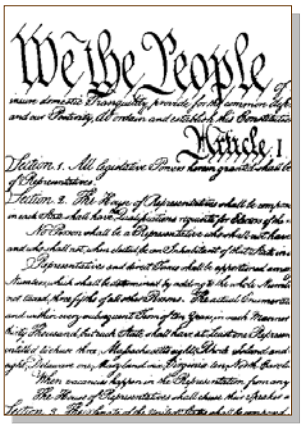
- **Identify, investigate, and report questionable activities**
- **Provide oversight of intelligence activities**
- **Determine if non-intelligence components are being used for foreign or counterintelligence purposes**
- **Ensure procedures exist for reporting questionable intelligence activities**

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Purpose of Intelligence Oversight

- **Enables military intelligence components to carry out their functions in a manner that protects the constitutional rights of U.S. persons.**
- **Regulates particular collection techniques to obtain information for foreign intelligence or counterintelligence purposes.**



66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Intelligence Oversight Applies To…

- **Named Military Intelligence components**
- **<u>Any</u> organization, staff, or office used for military intelligence purposes**
- **Both active and reserve components**
- **Members of the Army National Guard when performing Federal duties or engaging in activities directly related to a Federal duty or mission**
- **Contractors performing intelligence activities**

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Why Intelligence Oversight?

1960 & 1970s

Vietnam-era abuses:

- **Infiltration of college campuses**
- **Involvement in domestic political issues**
- **Surveillance of anti-war protestors**

→ **IO Mission**

The establishment of Intelligence Oversight has allowed military intelligence components to focus on their mission of collecting information related to *foreign* intelligence and counterintelligence purposes.

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Relevance in the 21st Century

GWOT DEPLOYMENTS	CONUS FORCE PROTECTION	EVOLVING CAPABILITIES
PRE-DEPLOYMENT TRAINING	INFORMATION FUSION Force Protection / Anti-Terrorism	OPEN-SOURCE INTELLIGENCE

Prevent "mission creep"

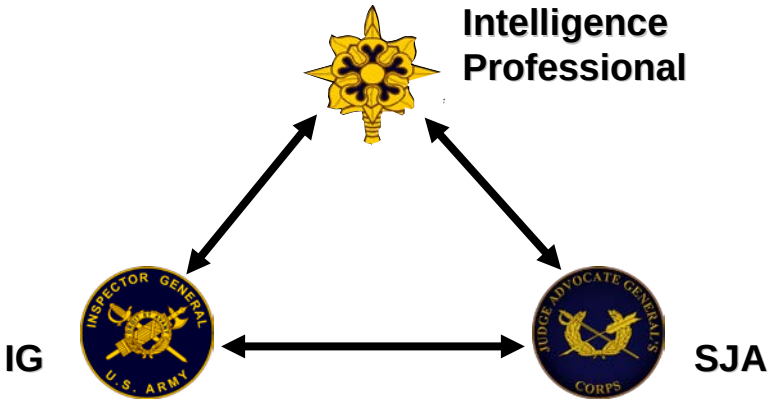
Protect Army interests

Protect constitutional rights

66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

Intelligence Oversight Triangle



66th Infantry Division Inspector General - INSPECTIONS BRANCH

INTELLIGENCE OVERSIGHT INSPECTION

General Inspection of the Intelligence Oversight Program

Inspection In-Briefing
Company B (MI)
1st Special Troops Battalion (STB)
20 July _____

66th Infantry Division Inspector General - INSPECTIONS BRANCH

Appendix F

Intelligence Oversight Training Scenario and Practical Exercises

1. **Purpose.** This appendix provides Inspectors General with a notional scenario and a variety of practical-exercise situations that they can use when conducting Intelligence Oversight inspections.

2. **Scenario Background.** You are a Military Intelligence (MI) officer / non-commissioned officer assigned to the 21st Infantry Division (Airborne), Fort Fremont, California. The division has a contingency mission to deploy to the island republic of Cortina to restore democracy in the event the current regime is overthrown. You are assigned to the 121st Military Intelligence (MI) Battalion as the OIC / NCOIC of the division Analysis Control Element (ACE). The ACE provides analytical support to the division G-2. Recently, you attended the weekly staff meeting in the G-2 office. LTC Alsorse, the division G-2, briefed the importance of force protection to the Division Commander -- especially in view of the recent bombing of the Federal Building in Sacramento. You briefed the current situation in Cortina and provided your assessment that an economic downturn, coupled with increased activity by the anti-U.S. Cortinian Liberation Army (CLA) in the mountainous interior of the island, increases the likelihood that the division may be deployed. Because of the tense situation caused by the bombing in Sacramento, getting the staff members' attention proved difficult -- especially in view of the Division Commander's guidance: "Get a handle on this, people. I don't want any bombings to happen here."

3. **Situation 1:** Upon returning to your office, you find a note from the G-2. He directs you to use all appropriate resources to obtain information on threats to the force. The G-2 wants to ensure that he is ahead of the power curve in the event that the Division Commander questions him. You call the ACE personnel together for a brainstorming session to determine the actions you can take to comply with the Division Commander's guidance. All agree that the first and most basic step to take is to search available on-line resources, both classified and unclassified, for threat information. SP4 Candu (MOS 96B), who is a whiz on the Worldwide Web, says that he will research unclassified sources. SSG Cipernette (MOS 35L) handles the searches on the classified systems. Later that afternoon, they return to you with the results of their searches:

- Cortinian dissidents are believed to have recruited a number of agents in the vicinity of Fort Fremont and the port at Oakland. Their mission is to provide early warning to the Cortinian Liberation Front in the event the division is mobilized.

- The Bear State Militia, a right-wing extremist group located in the rural north, has proclaimed the 21st Infantry Division to be an occupation force and has vowed to expel it from the State -- by force if necessary.

- SP4 Candu reports that he has also developed a list of IP addresses, email addresses, and URLs relating to Cortinian Support Groups. He wants permission to do more collection.

How do you handle this information? What Procedure(s) of AR 381-10 applies? What do they say? Are there any other offices / staffs / agencies that need to be involved? (Note: You may use any references available to you and consult with other unit personnel as you formulate a response. You must brief the IG on your solution prior to the completion of the inspection. You may bring any resources you desire to the briefing. You will have 10 minutes to brief your solution.)

IG Suggestion: Check out the HQDA Army G-2 Intelligence Oversight Web page at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html and the DoD Intelligence Oversight Web page at http://www.dod.mil/atsdio/.

Briefer: _____

Date / time / location: _____

HQDA, Army G-2 solution: Add the Cortinian information to your OB database. This information is legitimate intelligence data on a foreign intelligence capability. Procedure 1 applies because it's your mission. Pass the Bear State data to the Provost Marshal and USACIDC either verbally or in writing. If you write it, you can retain a copy in your administrative files (Military Correspondence Files). Do not add the information to intelligence databases. Make everyone involved read AR 525-13 so that they understand that U.S. domestic terrorism is not a Military Intelligence (MI) responsibility. You cannot retain this information EVEN IF IT'S OPEN-SOURCE MATERIAL!! The G-2 is not "database central" for all threats to the division.

The request to retain / collect on Internet addresses: All three categories (IP addresses, email addresses, and URLs) fall into the AR 381-10 framework. An IP address, without further information, does not identify or consist of information about a U.S. person. If further analysis on a specific IP is conducted, a reasonable and diligent inquiry must be conducted to determine if a U.S. person association exists. Email addresses are usually associated with an individual. Normally, the name will not provide sufficient information to identify the individual as a U.S. person. Sometimes, though, the name to the left of the "@" will provide persuasive evidence that the email address is associated with a U.S. person. The person may be a well-known public figure or the service provider may be closely affiliated with the U.S. Therefore, any email account should be presumed to be associated with a U.S. person. Once analysis begins, the component must make an effort to determine whether the addresses are

associated with U.S. persons. URLs specify the location of an object on the Internet, typically a Web page. The key factor to consider in determining whether a URL identifies a U.S person is the information to the right of the domain (the dot). Components may maintain URL addresses as long as the collection is within the scope of an authorized intelligence / counterintelligence activity. They may also open the Web sites associated with the URLs if part of an authorized mission. If the component wants to collect the information beyond what is available on the site, the component must determine whether the person about whom they are collecting is a U.S. person and, if so, comply with AR 381-10.

DAIG comment: No questionable activity if the Bear State Militia information is not used for intelligence purposes.

4. **Situation 2:** In response to command emphasis on Force Protection, you visit the local resident office of the supporting strategic counterintelligence (CI) group. This group, which has its headquarters at Fort Meade, has worldwide strategic CI responsibility for the Army. They advise you that they meet regularly with local authorities, to include the local office of the FBI, to exchange CI threat information. They appreciate the information you provided on CLF intelligence activity and assure you that they are on top of the situation. They also inform you that during a recent visit to the California Highway Patrol, they learned that some members of the Bear State Militia have come to believe that United Nations (U.N.) troops are using the Fort Fremont training area. These members believe that this alleged U.N. training situation is part of a larger conspiracy to put the U.S. under foreign control. They vow to march on Fort Fremont, locate the U.N. soldiers, and arrest and try them in the name of the Bear State. Six persons comprise the group, and they are armed.

How do you handle this information? What Procedure(s) of AR 381-10 applies? What do they say? Are there any other agencies / staffs / offices that need to be involved? (Note: You may use any references available to you and consult with other unit personnel as you formulate a response. You must brief the IG on your solution prior to the completion of the inspection. You may bring any resources you desire to the briefing. You will have 10 minutes to brief your solution.)

IG Suggestion: Check out the HQDA Army G-2 Intelligence Oversight Web page at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html and the DoD Intelligence Oversight Web page at http://www.dod.mil/atsdio/.

Briefer: _____

Date / time / location: _____

HQDA, Army G-2 Solution: Ask the CI folks if USACIDC and the division Provost Marshal have the information. If not, or if the CI folks don't know, decide which of you will tell them. But make sure you tell them!

Advise your G-2 of what you did and why (keep him or her informed and educated).

Do not add the information to intelligence databases or threat assessments.

DAIG comment: If the Provost Marshal notifies your MI unit that this group poses a threat to unit personnel, the unit may retain the information in Force Protection or physical security files but not in intelligence mission files. For example, you may not include this information in order-of-battle files. Situations 3 and 4 make similar points.

5. **Situation 3:** Following your visit to the supporting CI resident office, you return to find a note from LTC Alsorse, the division G-2. He has heard that the local Federal Bureau of Investigation (FBI) office is working to determine possible links between the Bear State Militia, other domestic terrorist groups, foreign agents, and individuals involved in area criminal activities. LTC Alsorse has received a request for support from the Special Agent in Charge (SAC) of the local FBI office for intelligence personnel with the skills to do this kind of predictive analysis work. LTC Alsorse wants to support them and is sure the Division Commander will agree since the information may help protect soldiers on Fort Fremont. He wants you to coordinate with the SAC and send over two soldiers right away -- "the sooner they start, the better."

How do you handle this information? What Procedure(s) of AR 381-10 applies? What do they say? Are there any other agencies / staffs / offices that need to be involved? (Note: You may use any references available to you and consult with other unit personnel as you formulate a response. You must brief the IG on your solution prior to the completion of the inspection. You may bring any resources you desire to the briefing. You will have 10 minutes to brief your solution.)

IG Suggestion: Check out the HQDA Army G-2 Intelligence Oversight web page at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html and the DoD Intelligence Oversight Web page at http://www.dod.mil/atsdio/.

Briefer: _____

Date / time / location: _____

Solution: Inform the G-2 that Procedure 12 requires that assistance provided by DoD intelligence component personnel to Federal law enforcement authorities must be coordinated with the service Office of the General Counsel for approval by OSD. Notify the local CI resident office and the Provost Marshal. If the local CI or PM office also received a request from the SAC, determine who might be the best element to provide the support, and ensure that that element gets the appropriate approval from HQDA and / or DoD.

6. **Situation 4:** During the weekly battalion staff meeting, you learn that some soldiers in another unit -- and in a different state -- confronted and killed a civilian couple who were walking in the vicinity of the installation. A subsequent investigation revealed that these soldiers were members of a white supremacist group, and their motivation was racial. The investigation also established that the soldiers had displayed distinctive tattoos and jewelry associated with their group prior to the killing. You learn that the Division Commander has reiterated his policy that he will not tolerate hate groups in his division. Later that day, the battalion CSM visits your section. He tells you that the Division Commander is charging all leaders on post, down to squad leaders and section chiefs, to identify soldiers who display logos and insignia associated with hate groups. You must report any such soldiers in your section to the appropriate Company Commander. To assist you in this requirement, the CSM gives you a pamphlet containing pictures of logos and insignia associated with hate groups along with a short summary of the group. The following is a typical entry:

The Bear State Militia: A right-wing extremist group dedicated to the "liberation" of California from Federal control. This group is loosely associated with a number of hate groups in California, to include white supremacist groups. The group is against everyone who is not of Northern European heritage and is particularly opposed to the use of any language but English outside the home. Members have been known to vandalize foreign-language signs and intimidate foreign-language speakers in public places. Their logo is a bear.

How do you handle this information? What Procedure(s) of AR 381-10 applies? What do they say? Are there any other staffs / offices that need to be involved? (Note: You may use any references available to you and consult with other unit personnel as you formulate a response. You must brief the IG on your solution prior to the completion of the inspection. You may bring any resources you desire to the briefing. You will have 10 minutes to brief your solution.)

IG Suggestion: Check out the HQDA Army G-2 Intelligence Oversight Web page at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html and the DoD Intelligence Oversight Web page at http://www.dod.mil/atsdio/.

Briefer: _____

Date / time / location: _____

HQDA, Army G-2 Solution: AR 381-10 does NOT apply. This activity is a normal command function governed by the 600-series regulations. MI units must comply with these regulations just like any other Army unit. Do it and report back through your chain of command. Do not file or use the information as intelligence. Instead, file the information in command administrative files (if you wrote the information down).

7. **Situation 5:** You receive through normal distribution a copy of the most recent Counterintelligence Appendix to the Intelligence Annex to the Division OPLAN. The appendix was prepared by CPT Bond, the CI Officer, and distributed directly from his office. You note that the format of the appendix has changed somewhat from the previous version. Now, under "Opposing Forces," there is a sub-section entitled "Local Threats." One of the paragraphs in this sub-section is the following:

- The Bear State Militia, a right-wing extremist group located in the rural north, has proclaimed that it considers the 21st ID to be an occupation force and has vowed to expel it from the State, using force if necessary. It also believes that the division is part of a larger conspiracy to put the U.S. under foreign, i.e., U.N., control. This group could interfere with road movements by the division if it believes the division is deploying to participate in U.N. operations.

How do you handle this information? What Procedure(s) of AR 381-10 applies? What do they say? Are there any other offices /staffs / agencies that need to be involved? (Note: You may use any references available to you and consult with other unit personnel as you formulate a response. You must brief the IG on your solution prior to the completion of the inspection. You may bring any resources you desire to the briefing. You will have 10 minutes to brief your solution.)

IG Suggestion: Check out the HQDA Army G-2 Intelligence Oversight Web page at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html and the DoD Intelligence Oversight Web page at http://www.dod.mil/atsdio/.

Briefer: _____

Date / time / location: _____

HQDA, Army G-2 solution: Notify CPT Bond and the unit Intelligence Oversight officer that the appendix appears to be in violation of AR 381-10, Procedure 1 (not your mission) because it's in violation of AR 525-13, paragraphs 2-17, 2-24, and 4-6 among others.

Report as questionable activity. Procedure 15 applies.

Notify the Provost Marshal so that he can include the information where appropriate in a non-intelligence annex.

8. **Situation 6:** As part of his planning guidance, the Division Commander informs his staff that he views the immediate disarming of the CLA as essential to the success of the division's mission to restore stability and democracy to Cortina. He wants as much information as possible on the CLA prior to deployment, to include full identification of the leadership, their names, backgrounds, attitudes toward U.S. forces, and current whereabouts. The G-2 translates the commander's information needs into priority intelligence requirements (PIR) for the ACE. As part of your intelligence preparation of the Cortinian battlefield, you begin to search all available resources for information on the CLA leadership. You quickly learn that several high-ranking members of the CLA are U.S. citizens or green-card holders who recently returned to Cortina to take up arms against the legitimate government. You also learn that one high-ranking member of the CLA, Yosep Calle, previously lived in the San Francisco area and is suspected of involvement in narcotics trafficking and money laundering.

How do you handle this information? What Procedure(s) of AR 381-10 applies? What do they say? Are there any other offices / staffs / agencies that need to be involved? (Note: You may use any references available to you and consult with other unit personnel as you formulate a response. You must brief the IG on your solution prior to the completion of the inspection. You may bring any resources you desire to the briefing. You will have 10 minutes to brief your solution.)

IG Suggestion: Check out the HQDA Army G-2 Intelligence Oversight Web page at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html and the DoD Intelligence Oversight Web page at http://www.dod.mil/atsdio/.

Briefer: _____

Date / time / location: _____

Solution: Refer to Procedure 2, AR 381-10. If you need the U.S. person information to accomplish your Cortinian mission, then you can collect it. Get a sanity check from your division Operational Law Attorney. Make sure the G-2 understands and agrees with your logic. Keep the division Provost Marshal informed on all criminal information; he is also a consumer of foreign intelligence. The U.S. persons who are in Cortina taking up arms are not legitimately of foreign intelligence interest.

9. **The Situation Continues:** The situation in Cortina continues to deteriorate. The government collapses. Two warring factions dominate the island. These factions are (1) the **Mainlanders** (descendents of immigrants from the mainland who controlled the now defunct government and dominate the economic and cultural life of the island and (2) the **Indiginees**, who are culturally and linguistically distinct from the Mainlanders. Many of the Indigenees see themselves as the rightful rulers of the island and resent the favored position of the Mainlanders. Others Indiginees are more favorably disposed to the Mainlanders and only want a voice in an ordered and democratic society. The situation is becoming increasingly polarized and the atrocities, in which both sides engage, are making reconciliation more difficult. Your division now deploys into this environment with the mission of keeping the warring factions apart while more moderate elements attempt to build a popular government and a stable society.

The G-2 expects the ACE to give the commander and staff a full picture of the attitudes and activities of both factions, to include what threat, if any, they may pose to the division, its mission, and its personnel. The MI battalion deploys IMINT, SIGINT, and HUMINT to meet these information needs; all sources begin providing valuable intelligence. The G-2 also expects the battalion CI assets to identify any attempt by the factions to collect on -- or infiltrate -- the division.

Because the division has very few members who can speak either of the two major Cortinian languages, the Army G-2 creates a local-hire program to provide interpreters and translators to the division. The CI team, with assistance from the Provost Marshal, G-1, and the supporting U.S. contractor, is tasked to pre-screen all applicants and weed out those individuals who may not be suitable for employment or might somehow pose a threat to the force. The CI team also sees this pre-screening activity as an opportunity to identify individual Cortinians who might assist in monitoring their colleagues; these Cortinians could identify and report attitudes or activities that might be inconsistent with employment by the division. Additionally, the CI team is tasked to report any positive intelligence incidentally obtained in accordance with the division collection plan. (HQDA, Army G-2 Note: All linguist acquisition falls under the purview of Army G-2 and is not a local matter. The Army is the DoD Executive Agent for managing DoD-wide linguist acquisition. Except for a very few Dari and Pashto linguists being recruited directly into the Individual Ready Reserve, a U.S. corporation under Army contract hires and manages all contract linguists.)

10. **Situation 7:** The division has now been in Cortina for four weeks and is set up in what had previously been a Cortinian Army compound. You are still the ACE Chief. Your analyst, SSG Cipernette, advises you that she has just received a spot report from the CI team. The report states that a local-hire employee reported that members of the Indiginee Liberation Army (ILA) and / or the Mainlander Defense Force (MDF) are contacting her and several of her co-workers in their homes and routinely debriefing them on the activities of U.S. Forces. You immediately contact CPT Bond, the division CI officer and acting G-2. He contacts the CI team and advises them of their responsibilities under AR 381-12, Threat Awareness and Reporting Program, to report this information through Army Theater Counterintelligence Coordinating Activities (ATCICA) channels to the Army Counterintelligence Coordinating Activity (ACICA). He also reminds you of the requirement in AR 381-12 to take no further action or make further dissemination unless directed or approved by the ATCICA or ACICA. After several days, you receive a response through ACICA channels: "The ACICA declines to open a case. Subject not under U.S. Army investigative jurisdiction. No further investigative activity authorized."

What do you do now? What options, if any, are open to you? How do you handle this information? What Procedure(s) of AR 381-10 applies? What do they say? Are there any other offices / staffs / agencies that need to be involved? (Note: You may use any references available to you and consult with other unit personnel as you formulate a response. You must brief the IG on your solution prior to the completion of the inspection. You may bring any resources you desire to the briefing. You will have 10 minutes to brief your solution.)

IG Suggestion: Check out the HQDA Army G-2 Intelligence Oversight Web page at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html and the DoD Intelligence Oversight Web page at http://www.dod.mil/atsdio/.

Briefer: _____

Date / time / location: _____

Solution: The key to this situation is correctly identifying the subjects, which, in this case, are the members of the ILA and MDF. You do not need investigative authorities to debrief your own employees or to collect on foreign activities in this situation. You should ensure that the division collection plan includes these requirements; that plan is your source of authority (see Chapter 6 of AR 381-20). If you suspect the local-hire employees of cooperating clandestinely with a local faction, the determination of whether to investigate them under the provisions of Chapter 4, AR 381-20, or collect on them under the provisions of Chapter 6, AR 381-20 (and / or division collection requirements), will depend upon the situation and should be made in consultation with supporting INSCOM elements in country (if any) and your Operational Law Attorney.

11. **Situation 8:** The G-2 is very pleased with the quality of information that his “INTs” are providing. The HUMINT teams are particularly productive, having built good relationships with key personnel in both factions. Each faction is eager to provide intelligence on the activities of the other -- particularly any intelligence that puts the other faction in a bad light. As time goes on, you notice that individual HUMINT team members are arguing among themselves over which faction really is “guilty.” They seem to have a psychological need to identify “good guys” and “bad guys.” This need seems strange to you because none of them has any pre-existing ties to Cortina or any of its factions. The attitudes of team members are entirely a result of relationships developed and information gathered since arrival on the island. This situation, while initially amusing, becomes serious when you learn that one of the HUMINT team members, SGT Arnold, MOS 35M, has passed -- on his own volition -- information to the MDF that one of the other team members obtained from the ILA. He made no secret of his intention to pass this information, stating to everyone within earshot that he was fed up with ILA terrorist activities. The information involved the leadership and organizational structure of the ILA and included the location of base camps, which the Indiginees provided to U.S. Forces with the understanding that the locations would not be disseminated outside of U.S. channels. The information was not otherwise classified. You notify the G-2, the division CI officer, and the MI Battalion Commander. The CI officer directs the CI team to submit a TARP report.

What options are open to the division, the Battalion Commander, and the G-2? What role should the division CI team play? What Procedure(s) of AR 381-10 apply? What do they say? Are there any other offices / staffs / agencies that need to be involved? (Note: You may use any references available to you and consult with other unit personnel as you formulate a response. You must brief the IG on your solution prior to the completion of the inspection. You may bring any resources you desire to the briefing. You will have 10 minutes to brief your solution.)

IG Suggestion: Check out the HQDA Army G-2 Intelligence Oversight Web page at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html and the DoD Intelligence Oversight Web page at http://www.dod.mil/atsdio/.

Briefer: _____

Date / time / location: _____

Solution: This situation illustrates a case that would appear to have no connection to Intelligence Oversight. In addition to the TARP report, the command could have also conducted a security investigation if classified information had been involved. The connection to Intelligence Oversight is the HUMINT team member's questionable activity during the conduct of intelligence activity under the provisions of Procedure 14, AR 381-10, and should be reported in accordance with Procedure 15, AR 381-10. As a

command versus an AR 381-10 issue, the team member's continued viability as a field HUMINTer demands further evaluation.

FOR TRAINING PURPOSES ONLY. ALL SCENARIOS AND PERSONS ARE FICTITIOUS.

Appendix G

Procedure 15 Reporting Format

1. **Purpose.** This appendix provides a format for reporting questionable activity through Procedure 15 up to DAIG's Intelligence Oversight Division (SAIG-IO).

2. **Questionable Activity.** A questionable activity is the violation of any law or regulation by personnel engaged in Military Intelligence activities and not simply violations of AR 381-10 (see Chapter 1). Any soldier actively engaged in a Military Intelligence activity and who violates an Army regulation while in the conduct of that activity constitutes a questionable activity. This questionable activity **must be reported to DAIG's Intelligence Oversight Division (SAIG-IO) within five days**. Procedure 15 reports are not punitive in nature but instead allow the Army to police Military Intelligence activities from within to avoid public embarrassment or breaches in public confidence. Violations of Army regulations may be punitive, however.

3. **Procedure 15 Reporting Format:** Procedure 15 reports may be in written (i.e., memorandum) or electronic format. The report should include the following items:

a. Identification of the personnel committing the alleged questionable activity by rank or civilian grade; security clearance and access; unit of assignment, employment, attachment, or detail; and assigned duties at the time of the activity. Do not identify individuals by name or other personal identifier unless the DCS, G-2 (DAMI-CDC) or TIG (SAIG-IO) so requests.

b. When and where the activity occurred.

c. A description of the activity and how it constitutes questionable intelligence activity. Cite the applicable portion(s) of AR 381-10 and other applicable law or policy.

d. Command and / or investigative agency actions planned or ongoing, if applicable.

4. Transmit reports via e-mail, facsimile, message, or hard copy as long as they meet the five-day requirement. An original signature is not required; electronic transmittal is the preferred method of delivery.

5. **Investigating a Questionable Activity:** Each report of questionable activity must be investigated to determine the facts necessary to assess whether the activity is legal and consistent with public policy. An IG Investigation is not required; a Commander's Inquiry or AR 15-6 investigation will suffice. When the investigation is complete, the investigating command must forward a copy of the final investigation report (with any disciplinary or corrective action taken) to SAIG-IO. The status of investigations exceeding one month in duration must be reported to SAIG-IO every **30 days** until complete.

Appendix H

Deputy Chief of Staff, G-2, Department of the Army Intelligence Oversight Inspection Checklist (dated19 February 2013)

1. **Purpose.** This appendix provides a copy of Army G-2's Intelligence Oversight Inspection Checklist as a guide for as IGs when planning for and executing Intelligence Oversight Inspections.

BACKGROUND INFORMATION

Date of Assessment:
Type of Assessment:
Organization:
Name of Intelligence Oversight Officer (IOO):
Name of Alternate:
Contact Information:
Mission of Unit:

INTERNAL ASSESSMENTS

1. Is Intelligence Oversight (IO) included in the unit's organizational inspection program (paragraph 1-4h(6), AR 381-10)?	YES	NO
Date of last organizational IO inspection:		
What were the findings or observations (attach report)?		
Were corrective actions taken?	YES	NO
What corrective actions were taken?		

NOTE: According to Department of the Army guidelines, an inspector has three levels that may be used to categorize findings. They are failing deficiency, deficiency, and observation. Areas highlighted in red on this checklist represent *potentially* failing deficiencies.

EXTERNAL INSPECTIONS

2. When was the last external IO inspection conducted?

Who conducted the inspection?

What were the results?

Were deficiencies addresses or corrected? YES NO

INTELLIGENCE OVERSIGHT OFFICER

3. Are intelligence oversight officers and alternates appointed in writing (paragraph 1-4p(4), AR 381-10)? YES NO

Are they appointed on orders signed by the commander of the unit? YES NO

Do the orders describe the essential duties of the IO officer? YES NO

Is an intelligence professional in the operational chain appointed as the IOO (paragraph 1-4p(4), AR 381-10)? YES NO

Note: The IO officer need not be assigned to the G-3 or S-3 but does need to be in a position with access to information on the unit's intelligence operations so that he / she can maintain oversight of these activities.

Are the IOOs duties reflected in the appropriate personnel evaluation support form? YES NO

Does the IOO have unfettered access to all programs, files, networks, and data necessary for the conduct of thorough and comprehensive oversight (paras 1-4h(7), 1-4i(6), 1-4j(7), 1-4k(6), 1-4m(6), and 1-4p(4), AR 381-10)? YES NO

Is the rank of the IOO commensurate with their responsibilities and the size of the unit? YES NO

INTELLIGENCE OVERSIGHT POLICY

4. Does the unit maintain an intelligence oversight policy book (maintained either online or as a paper document)? YES NO

Does the IOO have an understanding of the governing policies? YES NO

Are the following essential documents on hand? YES NO

Executive Order 12333, United States Intelligence Activities, Dec 81 (with amendment).

DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence components That Affect United States Persons, 7 Dec 82.

DoD Directive 5240.01, DoD Intelligence Activities, 27 Aug 07.

DTM 08-052, DoD Guidance for Reporting Questionable Intelligence Activities And Significant or Highly Sensitive Matters, 17 Sep 09, with Change 2, 22 Aug 11.

Army Regulation 381-10, U.S. Army Intelligence Activities, 3 May 07.

Army regulations, operations orders, command memoranda, or standing operating procedures (SOP) that authorize or relate to the mission and functions of the unit.

Unit intelligence oversight SOP.

If an INSCOM unit, are the following essential documents on hand? YES NO

Memorandum, INSCOM, IACO, subject: INSCOM Policy Memorandum #41

Memorandum, INSCOM, IACS, Subject: Intelligence Oversight (IO) Training for Contractors.

INTELLIGENCE OVERSIGHT TRAINING

5. Does the organization have an IO training program, with personnel receiving both initial and periodic refresher training (paragraph 14-1b, AR 381-10)?	YES	NO
How is the training delivered?		
Is the training tailored to the unit's mission?	YES	NO
How is the effectiveness of the training evaluated?		
Are incoming personnel receiving IO training within 30 days of arrival (paragraph 14-1b, AR 381-10)?	YES	NO
Are supporting contractors attending training (para 1-4p(3), AR 381-10)?	YES	NO
Are measures in effect to ensure personnel detailed outside the organization receive training?	YES	NO

REPORTING QUESTIONABLE INTELLIGENCE ACTIVITIES

6. Are internal procedures established to report questionable intelligence activities in accordance with Procedure 15?	YES	NO
Do personnel understand what must be reported in accordance with Procedure 15 (paragraph 15-4, AR 381-10)?	YES	NO
If questionable intelligence activities have occurred in the unit, are employees and supervisors reporting such activity upon discovery (para 14-2c and 15-2a, AR 381-10)?	YES	NO
Are Procedure 15 reports being sent to The Inspector General (TIG) within five days of discovery (para 15-2b, AR 381-10)?	YES	NO
Are employees aware that they have the option to submit Procedure 15 reports directly to TIG, the DCS G-2, the Army General Counsel, or other officials specified in para 15-2a, AR 381-10?	YES	NO
Has the unit generated any Procedure 15 reports in the last two years?	YES	NO
Are there indications that questionable intelligence activities have not been reported as required?	YES	NO
What measures has the unit taken to ensure that questionable intelligence activities previously reported as Procedure 15 do not continue to be a problem?		
Is the command conducting inquiries of questionable intelligence activity, when appropriate (paragraph 15-3, AR 381-10)?	YES	NO

COLLECTION OF U.S. PERSON INFORMATION

7. Does the mission of the organization involve the collection, retention, or dissemination of information on U.S. persons for intelligence purposes?	YES	NO
Is the unit collecting U.S. person information in accordance with its assigned mission and the policies of AR 381-10?	YES	NO
Does the unit's collection of U.S. persons information meet one of the categories defined in paragraph 2-2, AR 381-10?	YES	NO
Do IOOs and unit personnel understand that AR 381-10 does not itself authorize Intelligence activity (paragraph 1-5a, AR 381-10)?	YES	NO
If the unit collects U.S. person information as part of an assigned mission, what procedures are in place to ensure that such information is collected, retained, and disseminated in accordance with the policies of AR 381-10?		

ANNUAL FILES REVIEW

8. Does the unit conduct an annual review of intelligence files and databases in order to determine if retention of U.S. person information continues to be necessary to an authorized function of the unit (paragraph 3-3c, AR 381-10)?	YES	NO
What intelligence files does the unit maintain that contain information about U.S. persons?		
Do reviews of intelligence files and databases concentrate specifically on U.S. person information in order to determine if retention continues to be necessary to an assigned function of the organization (paragraph 3-3c, AR 381-10)?	YES	NO
What methodology is used to review the databases?		
Is there a document that verifies when the last annual review was accomplished?	YES	NO

INTELLIGENCE SUPPORT TO FORCE PROTECTION

9. Does the unit provide intelligence support to force protection?	YES	NO
If the organization is located in the U.S., is the collection of force protection information focused on data related to foreign intelligence and international terrorism (paragraph 17-1b, AR 381-10)?	YES	NO
If Military Intelligence (MI) elements providing support to force protection receive U.S. person information that is not retainable by an intelligence organization as specified in AR 381-10, is this information being passed to the appropriate law enforcement agency and not retained in intelligence files?	YES	NO
Are intelligence organizations controlling or maintaining force protection databases in the U.S. in contravention of AR 381-10 (paragraph 17-1g, AR 381-10)?	YES	NO

SPECIAL COLLECTION TECHNIQUES

10. Does the unit have the mission to employ special collection techniques as specified in Procedure 5 through 10, AR 381-10?	YES	NO
Is the unit employing special collection techniques in accordance with its mission and authorities?	YES	NO
If the unit has the mission and authority to employ special collection techniques, has each been approved at the level required in AR 381-10 or at the level delegated in writing by the proper authority?	YES	NO
Have requests for the use of special collection techniques been reviewed and approved, in writing, by proper legal authority?	YES	NO
Do operational personnel and supervisors understand and practice the "least intrusive means of collection" test before requesting approval for special collection Techniques (paragraph 2-3, AR 381-10)?	YES	NO
If a special collection technique has been authorized for a certain period of time, has the unit either requested an extension in writing or terminated the operation when that period has lapsed?	YES	NO
Note: The inspector should review documentation for special collection techniques that are both currently being employed and those that have been employed in the last several years, if the documentation is still available. Note on this report any questionable issues.		

USE OF BIOMETRIC EQUIPMENT

11. Does the unit maintain or use biometric equipment?	YES	NO
If yes, does the unit have a copy of DCS, G-2 Memo, Policy on Collection and Retention of Biometrics Data and Contextual Information in the United States by U.S. Army Military Intelligence Personnel, dated 15 Jan 09?	YES	NO
Do units with biometric equipment on hand include information on the permissible use of these devices in annual oversight training?	YES	NO
Are biometric devices in use in the U.S. being employed only for training purposes or as otherwise properly authorized?	YES	NO
Is biometric data gathered during training deleted at the end of each training session?	YES	NO
Are measures in place to prevent employees who have access to biometric databases from accessing biometrics data for unauthorized purposes?	YES	NO

CHECKLIST TAILORED FOR UNITS WITH CI MISSION

1. Are CI source operations and CI projects being properly documented in CI Special Operations Concepts (CISOC) prior to implementation? YES NO

2. Are CI source operations and CI projects being approved by proper authority at the level required by AR 381-10 prior to implementation? YES NO

3. Does the unit have established procedures for the periodic review of operations being executed under the purview of properly approved CISOCs? YES NO

4. Does the unit have the following CI related policy documents readily available for use by persons engaging in CI investigative or operational activities? YES NO

Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (FBI) (Delimitations Agreement), 1979

Supplement to 1979 FBI / DoD Memorandum of Understanding, Coordination of Counterintelligence Matters, 1 Apr 96

Memorandum of Understanding Between the FBI and DoD Governing Information Sharing, Operational Coordination, Investigative Responsibilities, 2 Aug 11

Annex A, Counterterrorism Information Sharing, to the Memorandum of Understanding Between the FBI and DoD Governing Information Sharing, Operational Coordination, and Investigative Responsibilities, 14 Mar 12

Annex B, Counterterrorism Information Sharing, to the Memorandum of Understanding Between the FBI and DoD Governing Information Sharing, Operational Coordination, and Investigative Responsibilities, 9 Dec 11

AR 381-12, Threat Awareness and Reporting Program (TARP), 4 Oct 10

AR 381-14 (C), Technical Counterintelligence (U), 30 Sep 02 (if appropriate)

AR 381-20 (S//NF), The Army Counterintelligence Program (U), 25 May 10

AR 381-47 (S//NF), Offensive Counterintelligence Operations (U), 17 Apr 06

AR 381-141 (C), Intelligence Contingency Funds (ICF) (U), 16 Jan 04 (if appropriate)

5. Do unit personnel understand CI investigative jurisdiction in both CONUS and OCONUS and do they know where to go for answers if they have questions (paragraphs 4-3 and 4-4, AR 381-20, and The Delimitation Agreement)? YES NO

6. Do unit personnel understand what constitutes misuse of badges and credentials and which of these matters are also reportable as Procedures 15 (paragraph 15-14, AR 381-20, and paragraph 15-4b (3), AR 381-10)? YES NO

CHECKLIST TAILROED FOR UNITS WITH A HUMINT MISSION

1. Does the unit have established procedures for the periodic review of all HUMINT operations to ensure compliance with policy and regulation?	YES	NO
2. Are Operational Proposals (OP) submitted for review and approval by proper authority before any HUMINT activity is conducted?	YES	NO
3. Are approved OPs current?	YES	NO
4. Are all Army HUMINT activities coordinated with the Army HUMINT Operations Center (AHOC), Army G-2X?	YES	NO
5. Is collection of U.S. person information done in accordance with the provisions of AR 381-10?	YES	NO
6. Do HUMINT collectors and support personnel understand what constitutes an IO reportable incident and how to report it?	YES	NO
7. Does the unit have the following documents readily available for use by persons conducting HUMINT activities?	YES	NO

DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning

DoDI S-3325.07, Guidelines for the Conduct of DoD Human Source Validation (U)

DoDD S-5200.09, Oversight, Management and Execution of Defense Clandestine Source Operations (U)

DoDD S-5200.37, Management and Execution of Defense Human Intelligence Activities (U)

DoDI C-5200.42, Defense Human Intelligence (HUMINT) and related Intelligence Activities (U)

DoDI 5205.01, DoD Foreign Military Intelligence Collection Activities (FORMICA)(U)

DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that affect U.S. Persons.

AR 381-10, U.S. Army Intelligence Activities

AR 381-100 (S), Army Human Intelligence Collection Programs (U)

DCS, G-2 Memo (S//NF), Interim Policy Guidance for the Conduct and Oversight of Army Human Intelligence (HUMINT) Source Operations (U)

AR 381-102 (S), U.S. Army Cover Support Program (U)

AR 381-141 (C), Intelligence Contingency Funds (ICF)(U)

DHE-M Vol. I 3301.001 (S//NF), Collection Requirements, Reporting, and Evaluation Procedures (U)

DHE-M Vol. II 3301.002 (S//NF), Collection Operations (U)

DA Pam 381-15 (S//NF), Foreign Military Intelligence Collection Activities Program (U)

FM 2-22.3, Human Intelligence Collector Operations

8. Are all HUMINT activities conducted in accordance with the above policies and regulations? YES NO

9. Do HUMINT collectors have the proper training and certification to conduct the category of HUMINT activity assigned to them? YES NO

CHECKLIST TAILORED FOR UNITS WITH A SIGINT MISSION

1. What is the source of the unit's authority to engage in a SIGINT mission?

Does the unit provide SIGINT personnel to perform duty with an NSA element? YES NO

Does the unit conduct a national SIGINT mission delegated by an NSA element? YES NO

Does the unit Conduct an Army SIGINT mission, as approved by DIRNSA, under delegated SIGINT Operational Tasking Authority? YES NO

(NOTE: If answers to the last two questions are no, skip to question 18)

2. If the unit is currently conducting a SIGINT mission, is their authority to do so specified in valid authority documentation that is on file)USSID / Site Profile, Mission Delegation Form (MDF), and Staff Processing Form (SPF))? YES NO

3. Are the unit's entries in NSA's SIGINT Address Book (SAB) and Goldpoint database correct? YES NO

4. Is the unit commander aware of his / her IO responsibilities as directed by USSID SE1000 Annex A? YES NO

Are the unit commander and senior leaders included in SIGINT IO awareness training provided by the Intelligence Oversight Officer (IOO)? YES NO

5. Does the organization have a primary and alternate IOO for SIGINT operations (USSID SE1000 Annex A) YES NO

Are the IOOs actively involved in the unit's SIGINT mission? YES NO

Are the primary and alternate IOOs commissioned officers, warrant officers, or NCOs in the grade of E-6 or above? YES NO

Are primary and alternate IOOs appointed on orders signed by the commander? YES NO

Are the IOOs knowledgable of their responsibilities as directed in USSID SE1000 Annex A? YES NO

6. If able to access an NSANet or JWICS workstation, have SIGINT IOOs completed OVSC2201 Intelligence Oversight Officer Training? (Note: this requirement is in addition to OVSC1000, OVSC1100, and OVSC1800 courses that are required for everyone).	YES	NO
7. Where practical, is there a SIGINT IOO present at all locations where the unit is engaging in a SIGINT mission?	YES	NO
In locations where a SIGINT IOO is not present, has the parent organization provided adequate IO training and oversight?	YES	NO
Does the SIGINT IOO interface regularly with these teams?	YES	NO
8. Does the SIGINT IOO maintain a binder or continuity book, in either paper or electronic format, to aid in transitions from outgoing to incoming IOOs?	YES	NO
9. If the unit is currently conducting a SIGINT mission, has it submitted an Oversight Implementation Report (OIR) via Army Cryptologic Operations (ACO) to the NSA / CSS SID Oversight and Compliance Office (SV)?	YES	NO
10. Has the unit submitted any SIGINT related incident reports in the last year?	YES	NO
If yes, were the reports submitted to all required offices (NSA IG, SID SV, and ACO)?	YES	NO
Was the commander aware of these reports, and was he involved in mitigation procedures?	YES	NO
Was a summary of the incident included in the quarterly IO report?	YES	NO
Has the unit failed to report any SIGINT related IO matter?	YES	NO
11. Has the unit submitted quarterly IO reports to ACO (and any other required offices)?	YES	NO
Were the reports submitted within seven days following the end of each quarter?	YES	NO
Were the reports signed by unit leadership (commander, S-2, or ACE Chief)?	YES	NO
Does the SIGINT IOO brief the contents of the reports to unit leadership prior to submitting them to ensure their complete knowledgeability?	YES	NO
Does the unit maintain copies of signed reports on file for at least three years?	YES	NO

NOTE: Units are required to submit formal reports only during those quarters when they have conducted SIGINT operations; otherwise an "NTR" via phone or email is acceptable.

12. If the unit has a SCIF, does the SIGINT IOO have access either to current paper copies, links to online versions, or readily accessible files on their computers of the following documentation? (Note: Only the NSA / CSS SID Policy Office may post USSIDs on-line.)

USSID SE1000, 11 May 12	YES	NO
USSID SE1000 Annex A 6 Dec 11	YES	NO
USSID SE1200, 15 Aug 12 (or other appropriate overarching USSID)	YES	NO
USSID SP0018, 25 Jan 11	YES	NO
USSID SP0019, 13 Nov 12	YES	NO
DCS, G-2 Memo, Interim Policy for Intelligence Oversight of Army Signals Intelligence (SIGINT) Operations, 29 Oct 10	YES	NO
NSA / CSS Policy 1-23, 29 May 09, and classified annex to DoD 5240.1-R. 16 Sep 11	YES	NO
Identities in SIGINT Manual, 12 Jan 12	YES	NO
NSCID 6, 17 Feb 72	YES	NO

13. If able to access an NSANet or JWICS workstation, have all personnel conducting, supervising, or managing SIGINT operations received the following required on-line IO training?

OVSC1000, NSA / CSS Intelligence Oversight Training	YES	NO
OVSC1100, Overview if Signals Intelligence Authorities	YES	NO
OVSC1800, Legal Compliance and Minimization Procedures	YES	NO

14. Are commanders and other senior leaders knowledgeable of IO for SIGINT operations that is appropriate for their level of leadership? YES NO

15. Have all personnel received annual IO training as required by AR 381-10? This training includes awareness of EO 12333, DoD Regulation 5240.1-R, and Procedures 1 to 4 and 14 to 15 in AR 381-10. YES NO

16. Do authorized personnel currently access raw SIGINT databases?	YES	NO
If required, are qualified primary and alternate auditors assigned and available?	YES	NO
Have auditors received OVSC3101 on-line training? (This training is in addition to OVSC1000, OVSC1100 and OVSC1800)	YES	NO
Are auditors able to describe and demonstrate their responsibilities in accordance with USSID CR1610?	YES	NO
Are procedures in place to terminate a person's databases access when such access is no longer required?	YES	NO
17. Does the unit task targets?	YES	NO
Are proper checks for foreignness conducted prior to tasking?	YES	NO
Are any checks for foreignness conducted thereafter?	YES	NO
18. Does the unit issue SIGINT reports or products?	YES	NO
Are proper sanitization or minimization procedures incorporated into pre-release quality control?	YES	NO
Are SIGINT reports reviewed after release for sanitization or minimization concerns?	YES	NO
19. Has the units IO program for SIGINT been subjected to prior inspections or staff assistance visits? Has the unit conducted inspections of its own operations?	YES	NO
20. Has the unit developed or employed any IO initiatives related to its SIGINT mission (for example, training tools, SOP, policy letters, or procedural guidelines)?	YES	NO
21. Do unit personnel understand the basic principles of IO?		
Why IO is important?	YES	NO
Why there is a need for oversight in the intelligence community?	YES	NO
Why IO is important for the Army?	YES	NO
What constitutes a U.S. person?	YES	NO
Who their SIGINT IOO is?	YES	NO

22. Do personnel engaging in SIGINT activities have access to the documents described in paragraph 12, above?	YES	NO
23. Test the ability of unit personnel to define what types of incidents would constitute reportable matters.		
24. Do personnel understand the mechanics for submitting a SIGINT related incident report, including the timelines for reporting?	YES	NO

CHECKLIST TAILORED FOR INTELLIGENCE UNITS ENGAGED IN COLLECTING, RETAINING, AND DISSEMINATING PUBLICALLY AVAILABLE INFORMATION

1. Does the unit's mission involve the acquisition of publically available information (paragraph 1-5d, AR 381-10)?	YES	NO
2. Can the information be acquired without special legal authorizations, such as court orders, search warrants, or approval of special collection techniques or operational concepts?	YES	NO
3. If the unit is collecting U.S. person information, does it have a legitimate mission to collect this information and does collection comply with the requirements of Procedure 2, AR 381-10 (paragraph 1-5d, AR 381-10)?	YES	NO
4. Has any requirement to disclose affiliation with the intelligence community been identified and addressed in accordance with Procedure 12, AR 381-10?	YES	NO
5. Does the collection comply with the obligations not to focus on a person solely because of race, ethnicity, national origin, religion, or the First Amendment rights of free speech and assembly (paragraph 2-5, AR 381-10)?	YES	NO
6. Is the method of collection authorized and appropriate to the mission of the unit?	YES	NO
7. Is the information being retained and disseminated in accordance with Procedure 3 and 4, AR 381-10?	YES	NO
8. If the unit is engaging in collection from Internet sources in which access to the public is meaningfully restricted, is this activity being accomplished by authority of an approved CISOC (para 8-8c, AR 381-10)?	YES	NO
9. If the unit is using non- or mis-attributable Internet access provided by a commercial Internet service provider, has the authority to do so been properly documented in accordance with para 1-9b, AR 381-10 and DCS, G-2 Memo (S//NF), subject: Nonattributable Internet Access (U), dated 17 Dec 07??	YES	NO