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
April 2004

**The Intelligence Oversight Guide**
**Table of Contents**

*Introduction*

**Chapter 1 - Background Information**

**Chapter 2 - Intelligence Oversight Inspection Methodology**

**Appendix A - Summary of AR 381-10 Procedures**

**Appendix B - Army G-2 / The Inspector General Message: Oversight of Intelligence Activities**

**Appendix C - Secretary of Defense Message / Army G-2 Memorandum: Intelligence Support to Force Protection**

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

**Appendix E - Intelligence Oversight Training Scenario and Practical Exercises**

**Appendix F – Procedure 15 Reporting Format**

# 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**. DAIG's Training Division (SAIG-TR) 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

DAIG's Training Division 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. **Updates.** DAIG's Training Division will distribute updated versions of this guide as necessary. The Training Division will notify -- and then forward electronic copies to -- all IG offices when changes have occurred.

7. **Summary of Updates.** This version of the guide now includes an appendix (Appendix F) that provides a format for Procedure 15 reports.

# 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 collect aggressively 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 D). 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 the ongoing war on terror. 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.

3. **The Intelligence Oversight System.**

a. **Standards.** Executive Order 12333 is the current Intelligence Oversight executive order. The Department of Defense implemented and amplified that executive order in Department of Defense (DoD) Directive 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons. Army Regulation (AR) 381-10 implements the DoD Directive. U.S. Signal Intelligence Directive (USSID) 18 provides further procedures for those intelligence components involved in signals intelligence. 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 G-2 (formerly the Deputy Chief of Staff for Intelligence, or DCSINT) is the policy proponent for AR 381-10. The chapters in AR 381-10 outline 15 procedures 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 (Identifying, Investigating, and Reporting Questionable Activities). Appendix A to this guide contains summaries of the AR 381-10 procedures. Electrical message, HQDA, DAMI-CI, 230900Z December 1994, Oversight of Intelligence Activities, expanded the role of DAIG and changed the reporting channels for questionable activities (but not Federal crimes). A copy of the message is at Appendix B.

(1) **Applicability.** AR 381-10 applies to all Army intelligence components and military and civilian employees of the Army when they engage in intelligence activities. AR 381-10 defines intelligence activities as all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333. Executive Order 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." These activities include S-2 shops and installation security offices when they perform intelligence functions. The regulation also 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 law-enforcement activities, including civil-disturbance activities undertaken by an intelligence component.

(2) **Responsibilities.** Every level of government, and each individual involved in intelligence activities, is charged with ensuring that those activities are conducted properly.

(a) **Individuals.** Each individual must:

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

- Conduct intelligence activities strictly in accordance with law, regulation, and policy.

- Report any suspected questionable activity in accordance with Procedure 15 of AR 381-10.

(b) **Commanders.** Commanders are responsible to ensure that:

- Personnel are familiar with the appropriate portions of AR 381-10.

- Intelligence activities are conducted in accordance with law, regulation, and policies.

- Employees report possible violations of AR 381-10.

- Possible violations of AR 381-10 are investigated and appropriate corrective action is taken.

- Intelligence Oversight personnel have full access to all appropriate information about intelligence activities.

(c) **Inspectors General.**

(aa) 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 Procedures 1 through 4 and 14 and how to report questionable activities under Procedure 15.

(bb) AR 381-10 charges IGs to:

- Determine, as part of their Intelligence Oversight responsibilities and in accordance with Procedure 15, whether intelligence components are involved in questionable activities.

- Determine whether any organization, staff, or office within their respective jurisdiction, but not otherwise specifically identified as a DoD intelligence component, is being used for foreign or counterintelligence purposes and, if so, ensure that the activities are in compliance with Executive Order 12333, DoD Directive 5240.1-R, and AR 381-10.

- Ensure that procedures exist within intelligence components for the reporting of questionable activities and that employees are aware of their responsibility to report such activities.

- Conduct investigations of possible questionable activities by intelligence personnel when directed by the Army General Counsel (OGC) through The Inspector General (TIG).

(d) **Legal Counsels.** OGC shares responsibility for Intelligence Oversight with the 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 the 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.

(e) **Army G-2.** Establishes Intelligence Oversight policy within the Army and serves as the proponent for AR 381-10.

(3) **Reporting.**

(a) **Questionable Activities.** Procedure 15 obligates all DoD employees to report any conduct, by an individual or an entity, that constitutes -- or is related to -- an intelligence activity that may violate the law, any executive order or Presidential directive, or any applicable DoD policy. Units should forward all reports of questionable activity through command channels to DAIG (SAIG-IO). Allegations of questionable activity must be reported 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 (DAIG), the Army G-2, or OGC. **Units must forward questionable-activity reports no later than five working days after discovery (see Appendix F**

**for the reporting format).** TIG forwards reports of questionable activity through OGC to the Assistant to the Secretary of Defense - Intelligence Oversight (ATSD-IO). The reporting policies directed by Procedure 15 are specifically designed to ensure that only questionable activities are reported to 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.

(b) **Federal Crimes by Intelligence Personnel.** Procedure 15, 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 statute or a Federal criminal statute. 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. Forward reportable Federal crimes to the Army G-2.

(c) **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 3b (1), requires specified major commands to provide input for this report to TIG.

# 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. 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. The Intelligence Oversight Division (SAIG-IO) of the U.S. Army Inspector General Agency (DAIG) 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.** 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. The inspection must identify any questionable activities; determine how violations are reported; and, if necessary, report violations found during the inspection. 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.** To identify intelligence components and personnel performing intelligence functions, ask the following questions: Where are the numbered Military Intelligence (MI) 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) performing intelligence functions? Some of these dual-hatted personnel may not realize that they are subject to the provisions of AR 381-10.

b. **Intelligence Oversight programs.** Some intelligence components develop formal Intelligence Oversight programs and assign Intelligence Oversight responsibilities to individual units. Current Army regulatory requirements do not require the establishment of such formal programs, however. If a unit has a formal Intelligence

Oversight program, that program should be tailored to the function and mission of the unit. Some items an Intelligence Oversight program should address are the frequency of Intelligence Oversight training (tailored to mission requirements); 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; a method for documenting training; and someone (or some office) formally responsible for reporting questionable activities. Usually, designated Intelligence Oversight officers are part of a formal Intelligence Oversight program. 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.

c. **Intelligence Oversight education.** AR 381-10, Procedure 14, paragraph b 2 requires personnel to be familiar with Procedures 1 through 4, 14, and 15. All personnel assigned to intelligence components must know that AR 381-10 prohibits intelligence components from collecting, retaining, or disseminating U.S. person information without the proper 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 E for an Intelligence Oversight training scenario and practical exercises.

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, 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.

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.

b. **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.

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

(1) Check to ensure that the unit has a copy (or has access to a copy via the Internet) of AR 381-10 and any applicable changes. Also check for any relevant Major Army Command (MACOM), Major Subordinate Command (MSC), or unit regulations or policies that require that intelligence components 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. A command or unit may require annual training on AR 381-10. 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) 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 E). 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.

(4) 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 come 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.

(5) 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).

(aa) 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. Military Intelligence does not have a mission to retain information on U.S. domestic threats; those threats are a law enforcement and Provost Marshal function (see Appendix C). The G-2 / S-2 is not involved in antiterrorism, 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.

(bb) Information retained for collection determination should not be over 90 days old or should have approval documentation for retaining it beyond 90 days. Some incidental U.S. person information may be in documents prepared by intelligence components outside your command, which does not necessarily violate AR 381-10 as long as the information is properly filed, does not refer to U.S. person information, and is not used to produce intelligence products.

(cc) 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.

(6) Check for an annual review of intelligence files. AR 381-10, Procedure 3, directs intelligence components to conduct an annual review of information in intelligence files. 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.

(7) Military Intelligence support to Law Enforcement Activities (LEA). 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 civilian LEA and the Federal Bureau of Investigation must come from the Office of the General Counsel. 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.

(8) Finally, determine if the intelligence component knows how to report a questionable activity in accordance with AR 381-10, Procedure 15. 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? Do they understand the IG role in Intelligence Oversight? Is the command Staff Judge Advocate (SJA) knowledgeable regarding Intelligence Oversight and the reporting of questionable activities? 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. 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 we uphold each individual's Constitutional rights and maintain the good name of the Army. 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 two primary questions that the component must answer are as follows: (1) What is your mission? and (2) What is your authority? Intelligence Oversight is usually a matter of individuals trying to do the right thing and not understanding the correct authority that governs their mission.

# Appendix A

## Summary of AR 381-10 Procedures

1. **Purpose.** This appendix provides a summary of the 15 Intelligence Oversight procedures outlined in AR 381-10.

2. **Procedure 1 – General Provisions.** Procedure 1 states 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. Participation of Department of the Army (DA) intelligence components in special activities is prohibited unless the President, Secretary of Defense, and Service Secretary have approved the special activity. Special activities are defined in Procedure 1. Assassinations are specifically forbidden as is requesting any other party to perform an act that the DA intelligence activity is prohibited from performing.

c. AR 381-10 does not apply to law enforcement activities, including civil disturbances. Procedure 12 requires Army General Counsel concurrence with support to civilian law enforcement agencies 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. Procedures 12 and 15 may also apply in the case of criminal information discovered by intelligence components.

3. **Procedure 2 - Collection of information about U.S. Persons.**

a. The core tenet of AR 381-10 is that a Department of Defense (DoD) intelligence component may collect information that identifies a U.S. person only:

(1) If the information is necessary to the conduct of a function assigned to that component, and

(2) The U.S. person falls into one of the 13 categories listed in Procedure 2.

b. The definition of collected can cause problems. AR 381-10, Procedure 2, paragraph b1, defines collection as follows: When employees of an intelligence component receive the information for use in the course of their official duties such as filing it or using it for the production of an intelligence report. If the employee simply passes the information on to another agency with responsibility for the issue, then the employee or unit did not collect the information.

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 DoD intelligence component to have been lawfully admitted into the U.S. for permanent residence,

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

(4) A U.S. corporation directed and controlled by U.S. citizens or permanent resident aliens.

d. Within the U.S. only, overt means may be used to collect foreign intelligence information on U.S. persons unless stringent tests are met as specified in paragraph d, Procedure 2.

e. When authorized to collect information on a U.S. person, intelligence components must still use the least intrusive collection means possible. Only when information cannot be gained from open sources will more intrusive means be used.

4. **Procedure 3 - Retention of Information About U.S. Persons.**

a. Information is defined as retained only if it can be retrieved by name or other identifying data.

b. U.S. person information may be retained only if it meets one of the following criteria:

(1) Information may be retained if it was properly collected under Procedure 2.

(2) The information was collected incidentally to authorized collection and

(a) Such information could have been collected under Procedure 2,

(b) Such information is necessary to understand or assess foreign intelligence or counterintelligence,

(c) The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with AR 381-10, or

(d) Such information may indicate criminal activities.

c. Access to U.S. person information will be restricted to certain individuals on a need-to-know basis. U.S. person information retained in intelligence component files will be reviewed annually in conjunction with the review required under AR 340-1 or AR 340-18-1. This review will determine whether continued retention serves the purpose for which it was collected and retained and that continued retention is necessary to the conduct of authorized functions of DA intelligence components or other government agencies.

4. **Procedure 4 - Dissemination of Information About U.S. Persons.**

Information that identifies U.S. persons may only be disseminated without the consent of those persons if the information was properly collected and / or retained under Procedures 2 and 3. The recipient must be reasonably believed to need the information for a lawful governmental function and be a member of one of the agencies listed in paragraph b2 of Procedure 4.

5. **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.

6. **Procedure 11 - Contracting for Goods and Services.**

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

b. DoD intelligence components 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 the activities of the DoD intelligence component.

7. **Procedure 12 - Provision of Assistance to Law Enforcement Authorities.**

a. Cooperation with law enforcement authorities by DA intelligence components must comply with DoD Directive 5525.5 and be for the purpose of:

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

(2) Protecting DoD employees, information, property, and facilities; and

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

b. DA intelligence components may provide the following types of assistance to law enforcement authorities:

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

(2) Specialized equipment and facilities may be provided when guidelines and approvals specified in DoD Directive 5525.5 are followed.

(3) Employees of DA intelligence components may be assigned to assist Federal law enforcement authorities when properly authorized and when the Army General Counsel concurs.

(4) Assistance may be provided to foreign governments and international organizations in accordance with applicable policies, laws, and treaties provided that no activities are undertaken against U.S. persons prohibited by AR 381-10.

8. **Procedure 13 - Experimentation on Human Subjects for Intelligence Purposes.**

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 or Deputy Under Secretary of Defense.

9. **Procedure 14 - Employee Conduct.**

a. Employees may only conduct intelligence activities in accordance with Executive Order 12333, AR 381-10, and other applicable laws and policies.

b. Each Army intelligence component must familiarize its employees with Executive Order 12333 and AR 381-10. At a minimum, the familiarization will cover Procedures 1 through 4, any other procedures applicable to the operations of the employee, and Procedure 15. The Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO) and each Inspector General is responsible for ensuring that this familiarization takes place.

c. The Secretary of the Army shall:

(1) Ensure that the Army General Counsel reviews any proposals for intelligence activities that may be contrary to law or policy.

(2) Protect persons reporting under Procedure 15 from reprisals.

(3) Impose appropriate punishment on individuals who violate AR 381-10.

(4) Recommend appropriate investigative action to the Secretary of Defense in cases involving serious breaches of security.

(5) Ensure that the Army General Counsel, Department of the Army Inspector General, DoD General Counsel, and Assistant to the Secretary of Defense for Intelligence Oversight have access to all information needed to perform their oversight responsibilities.

(6) Ensure that all employees cooperate fully with the White House Intelligence Oversight Board.

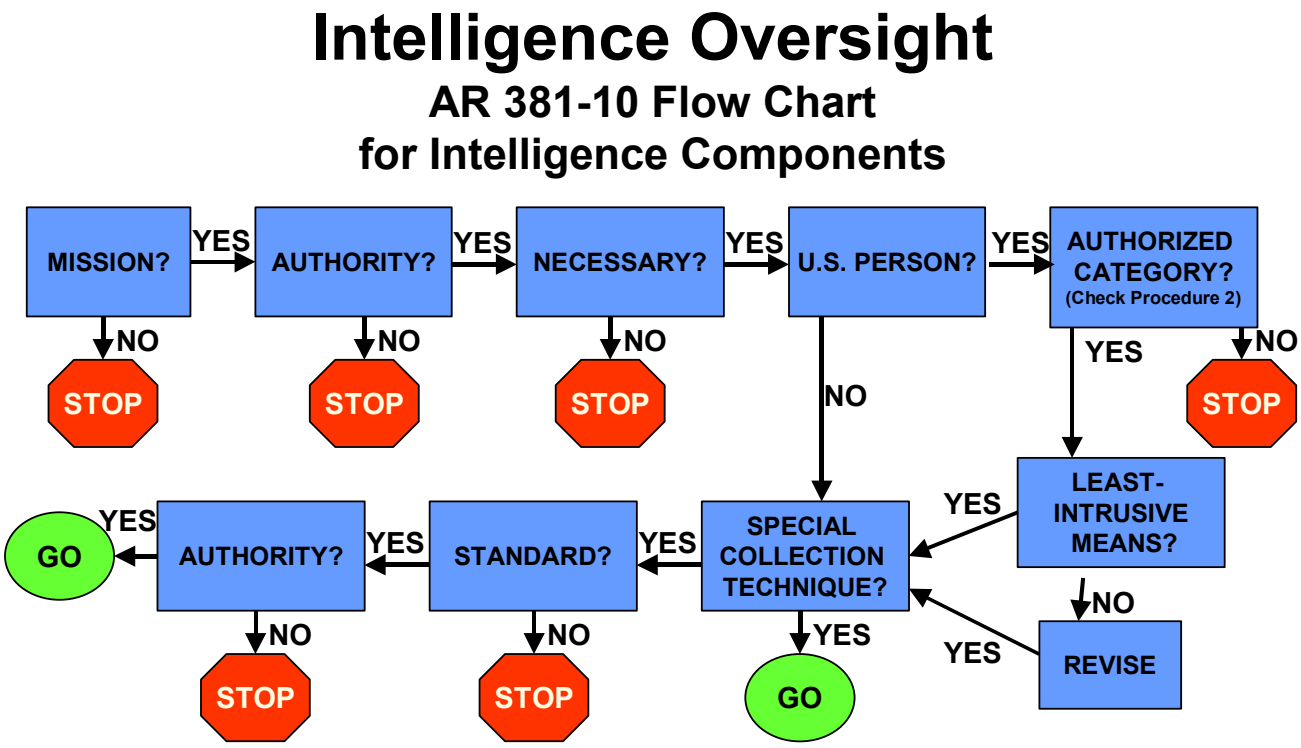
10. **Procedure 15 - Identifying, Investigating, and Reporting Questionable Activities.**

a. Each employee of a DA intelligence activity shall report any questionable activity to the General Counsel or Inspector General. A questionable activity is any conduct that constitutes -- or is related to -- an intelligence activity that may violate law, regulation, or policy. In practice this requirement means that employees must report both intelligence activities and conduct that may violate the law if that conduct is related to an intelligence activity. The operable question is “What is the intelligence activity?”

b. Reportable Federal crimes are reported to the HQDA Army G-2. DAIG receives all questionable-activity reports. If there is a question about where to report an allegation, contact the Army G-2 for a policy determination. For an explanation of the different types of reports, refer to the Frequently Asked Questions section on the Army G-2's Intelligence Oversight page (http://www.dami.army.pentagon.mil/offices/dami-ch/io/faq/faq.html).

c. The Inspector General (TIG) prepares a quarterly Intelligence Oversight report to the Assistant to the Secretary of the Army for Intelligence Oversight. The report includes a summary of unlawful or improper activities discovered, significant oversight activities, and recommendations for improvements to the program. Major Army Commands (MACOMs) and selected Direct Reporting Units (DRUs) will forward a quarterly report on significant intelligence activities and inspections to DAIG (SAIG-IO) not later than the fifth day following the end of the quarter.

11. **AR 381-10 Flow Chart.**



# Appendix B

## Army G-2 / The Inspector General Message: Oversight of Intelligence Activities

1. **Purpose.** This appendix provides a precise copy of the joint Army G-2 (then the Deputy Chief of Staff for Intelligence, or DCSINT) / The Inspector General message on Oversight of Intelligence Activities (dated 23 December 1994).

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

**MESSAGE, HQDA/DAMI-CI/SAIG-IO, 230900Z DEC 94, SUBJ: OVERSIGHT OF INTELLIGENCE ACTIVITIES**

R 230900Z DEC 94
FM HQ DA WASHINGTON DC//DAMI-CI/SAIG-IO//
TO AIG 12500
CDRINSCOM FT BELVOIR VA//IACS-IO/IAIG//
CINCUSAREUR HEIDELBERG GE//AEAGB-SA-IO/AEAIG//
CDRUSAEIGHT SEOUL KOR//EABJ-PL-S/EAIG//
CDRFORSCOM FT MCPHERSON GA//FCJ2-CI/FCIG
CDR650THMIGP SHAPE BE//ACSH-MI//
CDRUSARPAC FT SHAFTER HI//APIN-OC-CI//AOIG//
CDRUSARSO FTCLAYTON PM//SOIN/SOIG//
CDRUSASOC FT BRAGG NC//AOIN/AOIG//

SUBJ: OVERSIGHT OF INTELLIGENCE ACTIVITIES
1. REFERENCES.
A. DOD 5240.1R, 7 DEC 82, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFECT UNITED STATES PERSONS.
B. AR 10-5, 30 NOV 92, HEADQUARTERS, DEPARTMENT OF THE ARMY, ORGANIZATION AND FUNCTIONS.
C. AR 20-1, 15 MAR 94, INSPECTOR GENERAL ACTIVITIES AND PROCEDURES.
D. AR 381-10, 1 AUG 84, US ARMY INTELLIGENCE ACTIVITIES.
2. UNDER DIRECTION OF THE SECRETARY OF THE ARMY, THE INSPECTOR GENERAL OF THE ARMY (TIG) PROVIDES AN INDEPENDENT OVERSIGHT OF ALL ARMY INTELLIGENCE ACTIVITIES IN COORDINATION WITH THE OFFICE OF THE GENERAL COUNSEL (OGC) AND IN COMPLIANCE WITH APPROPRIATE LAWS, EXECUTIVE ORDERS AND REGULATIONS. THE DEPUTY CHIEF OF STAFF OF INTELLIGENCE (DCSINT) IS RESPONSIBLE FOR THE PROPRIETY OF US ARMY

INTELLIGENCE ACTIVITIES, IN COORDINATION WITH THE OGC AND WITH LEGAL ADVICE FROM THE JUDGE ADVOCATE GENERAL (TJAG). PROCEDURE 15, AR 381-10, CURRENTLY REQUIRES ALL ARMY PERSONNEL TO REPORT QUESTIONABLE INTELLIGENCE ACTIVITIES THROUGH INTELLIGENCE CHANNELS TO THE DCSINT. HOWEVER, IT HAS BEEN DETERMINED THAT THIS OVERSIGHT FUNCTION HERAFTER WILL BE PERFORMED BY TIG.
3. THE DEPUTY CHIEF OF THE STAFF FOR INTELLIGENCE (DCSINT) AND THE INSPECTOR GENERAL (TIG) OF THE ARMY RECENTLY SIGNED A MOA WHICH CHANGES PROCEDURE 15 REPORTING (AR 381-10) RESPONSIBILITIES FROM THE DCSINT TO TIG. THE MOA ALSO PROVIDES FOR THE REALIGNMENT OF ONE MILITARY INTELLIGENCE CIVILIAN EXCEPTED CAREER PROGRAM (MICECP) SPACE IN SUPPORT OF THIS FUNCTION. INSCOM WILL CHANGE THE PLACE OF DUTY FOR THE DETAILED MICECP EMPLOYEE FROM DCSINT TO TIG. THIS CHANGE IS EFFECTIVE 1 JANUARY 1995.
4. EFFECTIVE 1 JAN 95, THIS MESSAGE MODIFIES AR 381-10, PROCEDURE 15 REPORTING REQUIREMENTS AS FOLLOWS:
A. ALLEGATIONS OF QUESTIONABLE ACTIVITIES WILL NO LONGER BE REPORTED TO HQDA DCSINT (DAMI-CI). AS OF 1 JAN 95, ALL ALLEGATIONS OF QUESTIONABLE INTELLIGENCE ACTIVITIES WILL BE REPORTED TO TIG (SAIG-IO). CONTINUE TO USE THE FORMAT PROVIDED IN AR 381-10, PROCEDURE 15 FOR THE CONTENT OF THE REPORT.
B. MACOMS WILL ALSO CHANGE THE MESSAGE ADDRESS FOR THE QUARTERLY INTELLIGENCE OVERSIGHT REPORT FROM DAMI-CIC TO SAIG-IO. REPORTS CAN BE DONE IN MEMORANDUM FORMAT AND BE FAXED TO SAIG-IO AT STU III SECURE (703) 614-1867 OR NONSECURE DSN 225-7600. THIS REPORT IS DUE NOT LATER THAN 15 DAYS FOLLOWING THE CLOSE OF THE QUARTER. THE 1QFY95 REPORT COVERS THE TIME PERIOD FROM 1 OCT 94 TO 31 DEC 94 AND IS TO BE RECEIVED BY TIG (SAIG-IO) BY 15 JAN 95.
5. THIS MESSAGE DOES NOT CHANGE THE RESPONSIBILITY OF INTELLIGENCE COMMANDS TO ENSURE INTELLIGENCE ACTIVITIES ARE CONDUCTED PROPERLY; AND ARE COORDINATED WITH THEIR JUDGE ADVOCATE GENERAL IN ACCORDANCE WITH AR 381-10. THIS MESSAGE ALSO DOES NOT CHANGE FIELD IG OVERSIGHT RESPONSIBILITIES PER AR 20-1.
6. THIS IS A HQDA COORDINATED MESSAGE BY THE DCSINT, OGC, AND TIG. POC DCSINT IS MR. TED SNEDIKER (DAMI-CHI) DSN 227-3934; POC OGC IS MR. WHIT COBB DSN 227-8029; POC DAIG IS LTC FRANCES BELL/LTC CHARLES BORG (SAIG-IO) DSN 227-6630.

# Appendix C

## Secretary of Defense Message / Army G-2 Memorandum: Intelligence Support to Force Protection

1. **Purpose.** This appendix provides precise copies of the Secretary of Defense's message on Intelligence Support to Force Protection (dated 18 November 1998) and the Army G-2's (then the Deputy Chief of Staff for Intelligence, or DCSINT) memorandum on Policy Guidance for Intelligence Support to Force Protection in CONUS (dated 19 February 1999).

2. **Specific Text.**

a. The specific text of the Secretary of Defense message is as follows:

**MESSAGE, SECDEF/ATSD-IO, 181700Z NOV 98,**
**SUBJ: POLICY GUIDANCE FOR INTELLIGENCE SUPPORT TO FORCE PROTECTION**

UUUUU
P 181700Z NOV 98
FM SECDEF WASHINGTON DC//ATSD-IO//
TO RUEKJCS/JOINT STAFF WASHINGTON DC//OJCS-LA/DJS/IG/J2/J3//
RUEADWD/SECARMY WASHINGTON DC//SAIG-IO/GC//
RUENAAA/SECNAV WASHINGTON DC/NAVINSGEN/GC//
RUEAHQA/OSAF WASHINGTON DC//SAF-IGI/GC//
RUEADWD/CSA WASHINGTON DC//DACS/DAMI/DAJA/DAMO/DAAR//
RUENAAA/CNO WASHINGTON DC//N00/N09/N095/N2/N3/N5/NLSC//
RUEAHQA/CSAF WASHINGTON DC//CC/CV/XO/XOI/JAG/AF-RE//
RUEACMC/CMC WASHINGTON DC//CMC/ACMC/IG/SJA/CL/C4I/PP&O/MCRC//
RUFGNOA/USCINCEUR VAIHINGEN GE/IG/J2/J3/SJA//
RULYSCC/USACOM NORFOLK VA//IG/J2/J3/SJA//
RUCJACC/USCINCCENT MACDILL AFB FL//IG/J2/J3/SJA//
RUCJAAA/USSOCOM MACDILL AFB FL//IG/J2/J3/SJA/CORB//
RUMIAAA/USCINCSO MIAMI FL//IG/J2/J3/SJA//
RUPEUNA/USCINCSPACE PETERSON AFB CO//IG/J2/J3/SJA//
RHCUAAA/USCINCTRANS SCOTT AFB IL//IG/J2/J3/SJA//
RHHMUNA/USCINCPAC HONOLULU HI//IG/J2/J3/SJA//
RUCUSTR/USCINCSTRAT OFFUTT AFB NE//IG/J2/J3/SJA//
RUETIAA/DIRNSA FT GEORGE G MEADE MD//IG/GC/NSOC//

PAGE 02 RUEKJCS8619 UNCLAS
RUEKDIA/DIA WASHINGTON DC//IG/J2/GC/DO/DHS/DAC/DAJ/DIO/MC//
RUEBMJB/NRO WASHINGTON DC//IG/GC//
RUEAIJU/NIMA WASHINGTON DC//IG/GC//
RUEAADN/DTRA WASHINGTON DC//IG/GC/CI//
RUEAUSA/CNGB WASHINGTON DC//NGC-ZA/NCG-ARZ/NGB-IG//
RUEAUSA/NGB WASHINGTON DC//CF//
INFO RUEKJCS/SECDEF WASHINGTON DC//GC/IG/USDP/C3I/ATSD-IO//
RUDHAAA/CDRINSCOM FT BELVOIR VA//CDR/CS-IO/IG/DCSOPS/SJA//
RUCXNLG/ONI SUITLAND MD//IG/GC//
RUDHNIS/DIRNAVCRIMINVSERV WASHINGTON DC//IG/GC//
RUQVAIA/AIA KELLY AFB TX//CC/CV/IG/IN/SJA//
RUEDADI/AFOSI BOLLING AFB DC//CC/CV/IG/SJA//
RUWMFBA//AFIA KIRTLAND AFB NM//CC/IG-IO//
RULSMCA/MCIA QUANTICO VA
BT
UNCLAS SUBJECT: POLICY GUIDANCE FOR INTELLIGENCE SUPPORT TO FORCE PROTECTION
REFERENCES:
A. EXECUTIVE ORDER 12333
B. DODD 5240.1
C. DODD 5200.27
D. DOD REG 5240.1-R
E. MCM 75-91
F. AR 381-10
G. SECNAVINST 3820.3D
H. AFI 14-104
J. MCO 3800.2A
J. DIRECTOR OF COUNTERINTELLIGENCE MEMO, “AUTHORITY TO COLLECT INFORMATION ON DOMESTIC TERRORIST AND OTHER GROUPS COMMITTING ILLEGAL ACTS THAT POSE A THREAT TO THE DEPARTMENT OF DEFENSE (U),” DATED 27 JAN 98.
1. THE PURPOSE OF THIS MESSAGE IS TO PROVIDE POLICY GUIDANCE TO COMMANDERS AND SUPPORTING DODO INTELLIGENCE ORGANIZATIONS REGARDING PERMISSIBLE INTELLIGENCE SUPPORT FOR FORCE PROTECTION ACTIVITIES.
2. THIS MESSAGE HAS BEEN COORDINATED WITH THE JOINT STAFFF; THE DOD GENERAL COUNSEL; THE INSPECTOR GENERAL, DOD; THE UNDERSECRETARY OF DEFENSE FOR POLICY; AND THE SENIOR CIVILIAN OFFICIAL IN THE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE.
3. FORCE PROTECTION IS A FUNDAMENTAL COMMAND RESPONSIBILITY FOR ALL COMMANDERS WHEREVER LOCATED. DOD INTELLIGENCE AND COUNTERINTELLIGENCE (INTEL/CI) COMPONENTS HAVE AN IMPORTANT ROLE TO PLAY IN SUPPORT OF THE COMMANDERS’ FORCE PROTECTION MISSION.

EXECUTIVE ORDER 12333 AND DOD 5240.1-R REGULATE THE CONDUCT OF INTEL/CI ACTIVITIES; THE ATTORNEY GENERAL HAS APPROVED THE PROCEDURES IN DOD 5240.1-R. THEIR PURPOSE IS TO ENABLE DOD INTEL/CI COMPONENTS TO CARRY OUT EFFECTIVELY THEIR AUTHORIZED FUNCTIONS WHILE ENSURING THAT THEIR ACTIVITIES THAT AFFECT UNITED STATES PERSONS ARE CARRIED OUT IN A MANNER THAT PROTECTS THE CONSITITUTIONAL RIGHTS AND PRIVACY OF SUCH PERSONS.

4. INTEL/CI COMPONENTS DO NOT HAVE A LAW ENFORCEMENT MISSION. LAW ENFORCEMENT IS THE RESPONSIBILITY OF THOSE AGENCIES SPECIFICALLY CHARTERED TO HANDLE LAW ENFORCEMENT MATTERS, E.G., PROVOST MARSHAL; CID; OSI; AND NCIS. (NOTE: AFOSI AND NCIS HAVE BOTH COUNTERINTELLIGENCE AND LAW ENFORCEMENT MISSIONS, WHICH ARE MANAGED SEPARATELY WITHIN THESE ORGANIZATIONS.) OFF THE INSTALLATION IN CONUS, LAW ENFORCEMENT IS THE RESPONSIBILITY OF LOCAL AND STATE LAW ENFORCEMENT OFFICIALS AND THE FBI AT THE FEDERAL LEVEL, NOT DOD INTEL/CI COMPONENTS.

5. WHEN FOREIGN GROUPS OR PERSONS THREATEN DOD PERSONNEL, RESOURCES, OR ACTIVITIES – WHETHER CONUS OR OCONUS – DOD INTEL/CI COMPONENTS MAY INTENTIONALLY TARGET, COLLECT, RETAIN, AND DISSEMINATE INFORMATION ON THEM (UNLESS THE GROUPS OR PERSONS IN QUESTION MEET THE DEFINITION OF UNITED STATES PERSONS IN EXECUTIVE ORDER 12333/DOD 5240.1-R – SEE PARA 11A BELOW). BOTH CONUS AND OCONUS, INTEL/CI COMPONENTS ARE RESTRICTED IN WHAT AND HOW THEY CAN COLLECT, RETAIN, AND DISSEMINATE INFORMATION WITH RESPECT TO UNITED STATES PERSONS, AS EXPLAINED BELOW.

6. COMMANDERS MAY NOT LEGALLY DIRECT DOD INTEL/CI COMPONENTS TO TARGET OR INTENTIONALLY COLLECT INFORMATION FOR FORCE PROTECTION PURPOSES ON U.S. PERSONS UNLESS SUCH PERSONS HAVE BEEN IDENTIFIED IN REFERENCE J, OR SUBSEQUENT VERSIONS. THE FBI PARTICIPATES IN THE IDENTIFICATION OF THESE PERSONS.

7. COMMANDERS SHOULD BE COGNIZANT, HOWEVER, OF THE FACT THAT DURING THE CONDUCT OF ROUTINE LIAISON ACTIVITIES, DOD INTEL/CI COMPONENTS OFTEN RECEIVE INFORMATION IDENTIFYING U.S. PERSONS ALLEGED TO THREATEN DOD RESOURCES, INSTALLATIONS, MATERIEL, PERSONNEL, INFORMATION, OR ACTIVITIES. DOD INTEL/CI ACTIVITIES MAY ACT AS A CONDUIT AND MUST PASS ANY THREAT INFORMATION INCIDENTALLY RECEIVED IN THIS MANNER TO THE THREATENED COMMANDER AND THE ENTITY WHICH HAS RESPONSIBILITY FOR COUNTERING THAT THREAT (E.G., MILITARY POLICY, PROVOST MARSHAL, OR SECURITY DIRECTOR). THIS TRANSMITTAL OF INFORMATION DOES NOT CONSTITUTE COLLECTION BY THE DOD INTEL/CI CORGANIZATION WITHIN THE MEANING OF DOD REGULATION 5240.1-R (REFERENCE D), AND IS THEREFORE PERMISSIBLE. HOWEVER, ANY FOLLOW-ON INTEL/CI INVESTIGATION, COLLECTION, OR TARGETING OF SUCH U.S. PERSONS WOULD BE SUBJECT TO EXISTING PROCEDURES AS SET FORTH IN REFERENCES A THROUGH J.

8. IAW REFERENCE C., DOD LAW ENFORCEMENT AND SECURITY ORGANIZATIONS – AS OPPOSED TO INTEL/CI COMPONENTS – MAY LEGALLY ACCEPT AND RETAIN FOR UP TO 90 DAYS, UNLESS LONGER RETENTION IS REQUIRED BY LAW OR PERMISSION IS SPECIFICALLY GRANTED BY THE SECRETARY OF DEFENSE OR HIS DESIGNEE INFORMATION PERTAINING TO U.S. PERSONS WHICH THREATENS DOD RESOURCES, PERSONNEL, INSTALLATIONS, MATERIEL, INFORMATION, OR ACTIVITIES. COMMANDERS SHOULD TAKE APPROPRIATE ADVANTAGE OF LAW ENFORCEMENT LIAISION ACTIVITIES TO MONITOR CRIMINAL ACTIVITY IN THE VICINITY OF THEIR INSTALLATIONS/ACTIVITIES (ACTS OF TERROR, ASSAULT, THREATS OF HARM, OR DESTRUCTION OF GOVERNMENT PROPERTY ARE CRIMINAL ACTS).
9. TO CLARIFY THE ROLE OF DOD INTEL/CI ORGANIZATIONS IN SUPPORTING COMMANDERS' FORCE PROTECTION RESPONSIBILITIES, THE FOLLOWING GUIDANCE IS EFFECTIVE ON RECEIPT.
A. WHEN DOD INTEL/CI ORGANIZATIONS LEARN OF INFORMATION PRESENTING A REASONABLE BELIEF THAT A U.S. PERSON OTHER THAN A PERSON IDENTIFIED BY THE DOD DIRECTOR OF COUNTERINTELLIGENCE (IN REFERENCE J) POSES A THREAT TO DEPARTMENTAL RESOURCES, PERSONNEL, INSTALLATIONS, MATERIEL, INFORMATION, OR ACTIVITIES, THE ACQUIRING UNIT SHALL IMMEDIATELY ALERT THE APPROPRIATE OFFICIAL OF THE THREATENED ENTITY AND PROVIDE THE INFORMATION TO THE APPROPRIATE LAW ENFORCEMENT AUTHORITY. FOLLOWING SUCH NOTIFICATION, IF THE ACQUIRING UNIT HAS REASON TO PERMANENTLY RETAIN THAT INFORMATION UNDER THE PROVISION OF PROCEDURE 3 OF DOD REGULATION 5240.1-R, IT SHALL REQUEST, BY THE MOST EXPEDITIOUS MEANS AVAILABLE AND THROUGH ITS SERVICE INTELLIGENCE COMPONENT, THAT OASD(C3I) EVALUATE THE ACQUIRED INFORMATION FOR RETENTION ("COLLECTABILITY DETERMINATION"). OASD(C3I) WILL COORDINATE THE REQUEST WITH THE DOD GENERAL COUNSEL AND THE ATSD(IO) PRIOR TO NOTIFYING THE SERVICE INTELLIGENCE COMPONENT OF APPROVAL/DISAPPROVAL OF THE REQUEST. THE MILITARY SERVICES ARE ENJOINED TO PROCESS COLLECTABILITY DETERMINATIONS EXPEDITIOUSLY.
B. WHILE AWAITING A COLLECTABILITY/RETAINABILITY DETERMINATION, THE ACQUIRING UNIT MAY INDEX THE INFORMATION AND MAINTAIN IT ON FILE FOR A 90 DAY PERIOD. IF, DURING THAT 90 DAY PERIOD, THE ACQUIRING UNIT LEARNS OF ADDITIONAL INFORMATION RELATING TO THE THREAT POSED BY THE U.S. PERSON IN QUESTION, THE UNIT SHALL IMMEDIATELY PASS THAT INFORMATION TO THE APPROPRIATE OFFICIAL OR LAW ENFORCEMENT AUTHORITY. (THIS INFORMATION MAY BE DISSEMINATED TO AFFECTED COMMANDERS AND SECURITY OFFICIALS, ONLY.)
C. IF OASD(C3I) DENIES PERMISSION TO COLELCT OR RETAIN INFORMATION ON THE U.S. PERSON, THE REQUESTING ORGANIZATION WILL REMOVE ALL INFORMATION PERTAINING TO THAT U.S. PERSON FROM ITS FILES AND DESTROY IT OR TRANSFER IT TO A DOD LAW ENFORCEMENT OR SECURITY ACTIVITY WHICH HAS AN OFFICIAL NEED FOR THE INFORMATION. OASD(C3I) WILL PROVIDE TO OATSD(IO) AND THE GENERAL COUNSEL, WITHIN FIVE

WORKING DAYS, ONE COPY OF ALL PERMISSIONS TO COLLECT/RETAIN INFORMATION ON U.S. PERSONS NOT LISTED IN REFERENCE J. WITHIN 30 DAYS OF RECEIPT OF THIS MESSSAGE, HEADS OF DOD INTEL/CI COMPONENTS WILL PROVIDE TO OATSD(IO) ONE COPY OF ANY INSTRUCTIONS ISSUED WHICH IMPLEMENT THIS MESSAGE.

10. REQUEST HEADS OF DOD INTEL/CI COMPONENTS ENSURE THAT ALL FIELD LOCATIONS PROVIDING INTELLIGENCE SUPPORT TO COMMANDERS RECEIVE A COPY OF THIS MESSAGE.

11. ADDRESSEES ARE INVITED TO VISIT OUR RECENTLY ACTIVATED ATSD(IO) HOMEPAGE ON THE INTERNET AT HYPERLINK http://WWW.DTIC.MIL/ATSDIO WWW.DTIC.MIL/ATSDIO.

12. DEFINITIONS:

A. FROM APPENDIX A, DOD REGULATION 5240.1-R:

(1) THE TERM “U.S. PERSONS” MEANS:

(A) A U.S. CITIZEN;

(B) AN ALIEN KNOWN BY THE DOD INTELLIGENCE COMPONENT CONCERNED TO BE A PERMANENT RESIDENT ALIEN (PRA);

(C) AN UNINCORPORATED ASSOCIATION SUBSTANTIALLY COMPOSED OF U.S. CITIZENS OR PRAS;

(D) A CORPORATION INCORPORATED IN THE U.S., EXCEPT FOR A CORPORATION DIRECTED AND CONTROLLED BY A FOREIGN GOVERNMENT OR GOVERNMENTS. A CORPORATION OR CORPORATE SUBSIDIARY INCORPORATED ABROAD, EVEN IF PARTIALLY OR WHOLLY OWNED BY A CORPORATION INCORPORATED IN THE U.S., IS NOT A U.S. PERSON.

[A PERSON OR ORGANIZATION OUTSIDE THE U.S. SHALL BE PRESUMED NOT TO BE A U.S. PERSON UNLESS SPECIFIC INFORMATION TO THE CONTRARY IS OBTAINED. AN ALIEN IN THE U.S. SHALL BE PRESUMED NOT TO BE A U.S. PERSON UNLESS SPECIFIC INFORMATION TO THE CONTRARY IS OBTAINED.]

[A PERMANENT RESIDENT ALIEN IS A FOREIGN NATIONAL LAWFULLY ADMITTED INTO THE U.S. FOR PERMANENT RESIDENCE AND, THEREFORE, IS A U.S. PERSON.]

(2) FOREIGN INTELLIGENCE IS INFORMATION RELATING TO THE CAPABILITIES, INTENTIONS, AND ACTIVITIES OF FOREIGN POWERS, ORGANIZATIONS, OR PERSONS, BUT NOT INCLUDING COUNTERINTELLIGENCE EXCEPT FOR INFORMATION ON INTERNATIONAL TERRORIST ACTIVITIES.

(3) COUNTERINTELLIGENCE IS INFORMATION GATHERED AND ACTIVITIES CONDUCTED TO PROTECT AGAINST ESPIONAGE, OTHER INTELLIGENCE ACTIVITIES, SABOTAGE, OR ASSASSINATIONS CONDUCTED FOR OR ON BEHALF OF FOREIGN POWERS, ORGANIZATIONS, OR PERSONS, OR INTERNATIONAL TERRORIST ACTIVITIES, BUT NOT INCLUDING PERSONNEL, PHYSICAL, DOCUMENT, OR COMMUNICATIONS SECURITY PROGRAMS.

B. FROM JOINT PUB 2-01, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, DATED 23 MAR 94: FORCE PROTECTION IS DEFINED AS “SECURITY PROGRAM DESIGNED TO PROTECTSOLDIERS, CIVILIAN EMPLOYEES, FAMILY MEMBERS, FACILITIES, AND EQUIPMENT, IN ALL

LOCATIONS AND SITUATIONS, ACCOMPLISHED THROUGH PLANNED AND INTEGRATED APPLICATION OF COMBATING TERRORISM, PHYSICAL SECURITY, OPERATIONS SECURITY, PERSONAL PROTECTIVE SERVICES, AND SUPPORTED BY INTELLIGENCE, COUNTERINTELLIGENCE, AND OTHER SECURITY PROGRAMS."

UNCLASSIFIED

b. The specific text of the Army G-2 (formerly DCSINT) memorandum is as follows:

**MEMO, HQDA DCSINT, 19 FEB 99,**
**SUBJ: POLICY GUIDANCE FOR INTELLIGENCE SUPPORT TO FORCE PROTECTION IN CONUS**

DAMI-CHI (1oo) 19 Feb 99

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Guidance for Intelligence Support to Force Protection in CONUS

1. References:

a. AR 381-10, U.S. Army Intelligence Activities, 1 Aug 84.

b. AR 381-12, Subversion and Espionage Directed Against the Army (SAEDA), 15 Jan 93.

c. AR 381-20, The Army Counterintelligence Program, 15 Nov 93.

d. AR 525-13, Antiterrorism Force Protection (AT / FP): Security of Personnel, Information, and Critical Resources, 10 Sep 98.

e. DoD message, ATSD-IO, dtg 181700Z Nov 98, subject: Policy Guidance for Intelligence Support to Force Protection (enclosed).

2. Reference 1a governs Military Intelligence (MI) activities that affect United States Persons and states that authority to employ certain collection techniques is limited to that necessary to perform functions assigned to the intelligence component. References 1b-1d assign more specific functions and responsibilities for intelligence support to force protection. Reference 1e is the most current DoD guidance.

3. This memo implements reference 1e and provides additional guidance:

a. Although reference 1e refers to a DoD list of U.S. Persons and organizations against which DoD intelligence elements may collect, Army MI elements may not conduct intelligence activities specifically targeting them. Because the Army maintains its law enforcement separately from its intelligence elements, it is inappropriate to collect information on these persons and organizations through intelligence activities. The Army designated law enforcement as the responsible agency per reference 1d.

b. MI elements will no longer report U.S. criminal threat information as intelligence or SAEDA incident reports. This change is being included in the revision of references 1b and 1c. Note that this does not pertain to national security crimes (treason, spying, espionage, sedition, subversion, etc.), which are within MI responsibility per reference 1c.

c. MI personnel will pass, via the most expedient method, U.S. criminal and U.S. terrorist threat information received through normal assigned activities ("incidentally acquired") to the Provost Marshal / Director of Security and the U.S. Army Criminal Investigation Command (USACIDC). Receiving and passing the information fully complies with references 1a and 1e. Do not send copies to the HQDA Antiterrorism Operations and Intelligence Cell or Army Counterintelligence Center as it could create circular reporting or false confirmation. USACIDC has that reporting responsibility per reference 1d. A synopsis may be filed in general correspondence files ("administrative purposes") as needed for crediting work done.

d. MI personnel will refer requests for U.S. terrorist and U.S. criminal threat information and assessments to USACIDC or the Provost Marshal in accordance with reference 1d. Local threat assessments are the installation's responsibility; MI may augment the local information with foreign intelligence and counterintelligence information and analysis.

e. MI personnel participating in AT / FP assessment teams per reference 1d are responsible for foreign intelligence and counterintelligence information and analysis. They may provide analytical advice and assistance to other team personnel in developing the overall assessment but should not be used as the analytical subject-matter expert for non-MI functional areas.

f. Any MI element may request a collection determination through command channels to HQDA (DAMI-CHI) in accordance with references 1a and 1e. Because of the 90-day retention time limit in reference 1a, commanders must ensure speedy transmittal to HQDA.

4. This memo was coordinated with the Office of the Army General Counsel, Office of The Judge Advocate General, Office of The Inspector General, Office of the Deputy Chief of Staff for Operations, USACIDC, and the Intelligence and Security Command.

5. Ensure widest possible dissemination to commanders, operations personnel, installation security officials, provosts marshal, inspectors general, criminal

investigative, and intelligence elements. MACOM supplements require HQDA prior approval.

//original signed//
Encl CLAUDIA J. KENNEDY
Lieutenant General, GS
Deputy Chief of Staff
for Intelligence

DISTRIBUTION:
U.S. Army Corps of Engineers
U.S. Army Criminal Investigation Command
U.S. Army Forces Command
U.S. Army Intelligence and Security Command
U.S. Army Materiel Command
U.S. Army Medical Command
U.S. Military Academy
U.S. Army Military District of Washington
Military Traffic Management Command
National Guard Bureau
U.S. Army Pacific
U.S. Army Reserve Command
U.S. Army Space and Missile Defense Command
U.S. Army Special Operations Command
Third U.S. Army
U.S. Army Training and Doctrine Command
U.S. Army Intelligence Center and Fort Huachuca

CF:
ATSD-IO
SAGC
SAIG-IO
DAJA-IO
DAMO-ODL
Eighth U.S. Army
U.S. Army Europe and Seventh Army
U.S. Army South
650th Military Intelligence Group

# Appendix D

## 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:

**MEMO, HQDA DCSINT, 05 Nov 01,**
**SUBJ: Collecting Information on U.S. Persons**

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)
SAGC
SAIG-IO
DAJA-IO

# Appendix E

## 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 97B) 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 www.dtic.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 provide 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 www.dtic.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.

4. **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 www.dtic.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.

5. **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 www.dtic.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).

6. **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 www.dtic.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.

7. **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 www.dtic.mil/atsdio.

Briefer: _____

Date / time / location: _____

Solution: Refer to paragraph C.2.3, 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.

8. **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.)

9. **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, Subversion and Espionage Directed Against the U.S. Army (SAEDA), to report this information through sub-control-office channels to the Army Central Control Office. He also reminds you of the requirement in paragraph 3-4.b (3), AR 381-12, to take no further action or make further dissemination unless directed or approved by a control office. After several days, you receive a response through control-office channels: "The Control Office 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 www.dtic.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.

10. **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 97E, 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 SAEDA 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 www.dtic.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 SAEDA 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 F

## Procedure 15 Reporting Format

1. **Purpose.** This appendix provides a format for reporting questionable activity through Procedure 15 up to DAIG 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 working 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 should be in memorandum format and include the following items:

a. A description of the nature of the questionable activity.
b. The date, time, and location of the questionable activity.
c. The individual or unit responsible for the questionable activity.
d. A summary of the incident, to include references to particular portions of AR 381-10 if applicable.
e. Status of the investigation into the incident (see paragraph four below).

4. **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.