

**DEPUTY CHIEF OF STAFF, G-2, DEPARTMENT OF THE ARMY**

**INTELLIGENCE OVERSIGHT ASSESSMENT/INSPECTION**

**19 Feb 13**

BACKGROUND INFORMATION

Date of Assessment:

Type of Assessment:

Organization:

Name of Intelligence Oversight Officer:

Name of Alternate:

Contact Information:

Mission of Unit:

INTERNAL ASSESSMENTS

1. Is intelligence oversight included in the unit's organizational inspection program (para 1-4h(6), AR 381-10)?

YES NO

Date of last organizational IO inspection:

What were the findings or observations (attach report)?

Were corrective actions taken?

YES NO

What corrective actions were taken?

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

## EXTERNAL INSPECTIONS

2. When was the last external intelligence oversight inspection conducted?

Who conducted the inspection?

What were the results?

Were deficiencies addressed or corrected? YES NO

## INTELLIGENCE OVERSIGHT OFFICERS

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

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

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

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

Note: The IOO need not be assigned to the G-3 or S-3, but he does need to be in a position where he has access to information on the unit's intelligence operations so that he can maintain effective oversight of these activities.

Are the intelligence oversight officer's duties reflected in the appropriate personnel evaluation support form? YES NO

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

Is the rank of the IO officer commensurate with his responsibilities and the size of the unit? YES NO

## INTELLIGENCE OVERSIGHT POLICY

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

Does the IO officer have an understanding of what the governing policies are? YES NO

Are the following essential documents on hand? YES NO

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

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

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

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

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

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

Unit intelligence oversight SOP.

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

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

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

## INTELLIGENCE OVERSIGHT TRAINING

5. Does the organization have an intelligence oversight training program, with personnel receiving both initial and periodic refresher training (Para 14-1b, AR 381-10)?

YES NO

How is training delivered?

Is training tailored to the unit's mission?

YES NO

How is the effectiveness of training evaluated?

Are incoming personnel receiving intelligence oversight training within 30 days of arrival (para 14-1b, AR 381-10)?

YES NO

Are supporting contractors attending training (para 1-4p(3), AR 381-10)?

YES NO

Are measures in effect to ensure personnel detailed outside the organization receive training?

YES NO



## REPORTING QUESTIONABLE INTELLIGENCE ACTIVITIES

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

COLLECTION OF U.S. PERSON INFORMATION

7. Does the mission of the organization involve the collection, retention, or dissemination of information on U.S. persons for intelligence purposes? YES NO

Is the unit collecting U.S. person information in accordance with its assigned mission and the policies of AR 381-10? YES NO

Does the unit's collection of U.S. person information meet one of the categories defined in para 2-2, AR 381-10? YES NO

Do IO officers and unit personnel understand that AR 381-10 does not itself authorize intelligence activity (para 1-5a, AR 381-10)? YES NO

If the unit collects U.S. person information as part of an assigned mission, what procedures are in place to ensure that such information is collected, retained, and disseminated in accordance with the policies of AR 381-10?

## ANNUAL FILES REVIEW

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

## INTELLIGENCE SUPPORT TO FORCE PROTECTION

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



SPECIAL COLLECTION TECHNIQUES

10. Does the unit have the mission to employ special collection techniques as specified in Procedures 5 through 10, AR 381-10?

YES NO

Is the unit employing special collection techniques in accordance with its mission and authorities?

YES NO

If the unit has the mission and authority to employ special collection techniques, has each been approved at the level required in AR 381-10 or at the level delegated in writing by proper authority?

YES NO

Have requests for the use of special collection techniques been reviewed and approved, in writing, by proper legal authority?

YES NO

Do operational personnel and supervisors understand and practice the "least intrusive means of collection" test before requesting approval for special collection techniques (para 2-3, AR 381-10)?

YES NO

If a special collection technique has been authorized for a certain period of time, has the unit either requested an extension in writing or terminated the operation when that period has lapsed?

YES NO

Note: The inspector should review documentation for special collection techniques that are both currently being employed and those that have been employed in the last several years, if the documentation is still available. Note on this report any questionable issues.



## USE OF BIOMETRIC EQUIPMENT

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

## CHECKLIST TAILORED FOR UNITS WITH CI MISSION

- |  |     |    |
|--|-----|----|
| 1. Are CI source operations and CI projects being properly documented in CI Special Operations Concepts (CISOC) prior to implementation?                     | YES | NO |
| 2. Are CI source operations and CI projects being approved by proper authority at the level required by AR 381-20 prior to implementation?                   | YES | NO |
| 3. Does the unit have established procedures for the periodic review of operations being executed under the purview of properly approved CISOCs?             | YES | NO |
| 4. Does the unit have the following CI related policy documents readily available for use by persons engaging in CI investigative or operational activities? | YES | NO |

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

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

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

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

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

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

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

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

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

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

5. Do unit personnel understand CI investigative jurisdiction in both CONUS and OCONUS and do they know where to go for answers if they have questions (paras 4-3 and 4-4, AR 381-20 and The Delimitations Agreement)?

YES NO

6. Do unit personnel understand what constitutes misuse of badges and Credentials and which of these matters are also reportable as Procedure 15 (para 15-13, AR 381-20 and para 15-4b(3), AR 381-10)?

YES NO



## CHECKLIST TAILORED FOR UNITS WITH A HUMINT MISSION

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

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

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

DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations (U)

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

DoDI S-5200.42, Defense Human Intelligence (HUMINT) and Related Intelligence Activities (U)

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

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

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

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

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

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

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

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

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

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

FM 2-22.3, Human Intelligence Collector Operations

8. Are all HUMINT activities conducted in accordance with the above policies and regulations?

YES NO

9. Do HUMINT collectors have the proper training and certification to conduct the category of HUMINT activity assigned to them?

YES NO



## CHECKLIST TAILORED FOR UNITS WITH A SIGINT MISSION

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

Does the unit provide SIGINT personnel to perform duty with an NSA element?

YES NO

Does the unit conduct a national SIGINT mission delegated by an NSA element?

YES NO

Does the unit conduct an Army SIGINT mission, as approved by DIRNSA, under delegated SIGINT Operational Tasking Authority?

YES NO

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

2. If the unit is currently conducting a SIGINT mission, is their authority to do so specified in valid authority documentation that is on file (USSID/Site Profile, Mission Delegation Form (MDF), and Staff Processing Form (SPF))?

YES NO

3. Are the unit's entries in NSA's SIGINT Address Book (SAB) and Goldpoint database correct?

YES NO

4. Is the unit commander aware of his intelligence oversight responsibilities as directed by USSID SE1000 Annex A?

YES NO

Are the commander and other senior leaders included in SIGINT IO awareness training provided by the intelligence oversight officer (IOO)?

YES NO

5. Does the organization have a primary and alternate intelligence oversight officer for SIGINT operations (USSID SE1000 Annex A)?

YES NO

Are the Intelligence Oversight officers actively involved in unit's SIGINT mission?

YES NO

Are the primary and alternate IOOs commissioned officers, warrant officers, or NCOs in the grade of E-6 or above?

YES NO

Are primary and alternate IOOs appointed on orders signed by the commander?

YES NO



Are the intelligence oversight officers knowledgeable of their responsibilities as directed in USSID SE 1000 Annex A?	YES	NO
6. If able to access an NSANet or JWICS workstation, have SIGINT IOOs completed OVSC2201 Intelligence Oversight Officer training? (Note: this requirement is in addition to OVSC1000, OVSC1100, and OVSC1800 courses that are required for everyone).	YES	NO
7. Where practical, is there a SIGINT IOO present at all locations where the unit is engaging in a SIGINT mission?	YES	NO
In locations where a SIGINT IO officer is not present, has the parent organization provided adequate IO training and oversight?	YES	NO
Does the SIGINT IO officer interface regularly with these teams?	YES	NO
8. Does the SIGINT IOO maintain a binder or continuity book, in either paper or electronic format, to aid in transitions from outgoing to incoming IOOs?	YES	NO
9. If the unit is currently conducting a SIGINT mission, has it submitted an Oversight implementation report (OIR) via Army Cryptologic Operations (ACO) to the NSA/CSS SID Oversight and Compliance Office (SV)?	YES	NO
10. Has the unit submitted any Signals Intelligence related incident reports in the last year?	YES	NO
If yes, were the reports submitted to all requires offices (NSA IG, SID SV, and ACO)?	YES	NO
Was the commander aware of these reports and was he involved in mitigation procedures?	YES	NO
Was a summary of the incident or incidents included in the Quarterly IO report?	YES	NO
Has the unit failed to report any signals intelligence related intelligence oversight matter?	YES	NO

11. Has the unit submitted quarterly IO reports to ACO (and any other required offices)?

YES NO

Were these reports submitted within the seven days following the end of each quarter?

YES NO

Were the reports signed by unit leadership (the commander, S-2 officer, or ACE Chief)?

YES NO

Does the SIGINT IOO brief the contents of reports to unit leadership prior to submitting them to ensure their complete knowledgeability?

YES NO

Does the unit maintain copies of signed reports on file for at least three years?

YES NO

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

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

USSID SE1000, 11 May 12

YES NO

USSID SE1000 Annex A, 6 Dec 11

YES NO

USSID SE1200, 15 Aug 12 (or other appropriate overarching USSID)

YES NO

USSID SP0018, 25 Jan 11

YES NO

USSID SP0019, 13 Nov 12

YES NO

DCS, G-2 Memo, Interim Policy for Intelligence Oversight of Army Signals Intelligence (SIGINT) Operations, 29 Oct 10

YES NO

NSA/CSS Policy 1-23, 29 May 09, and classified annex to DoD 5240.1-R, 16 Sep 11

YES NO

Identities in SIGINT Manual, 12 Jan 12

YES NO

NSCID 6, 17 Feb 72

YES NO



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

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

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

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

16. Do authorized personnel currently access raw SIGINT databases? YES NO

If required, are qualified primary and alternate auditors assigned and available? YES NO

Have auditors received OVSC3101 on-line training? (This is in addition to OVSC1000, OVSC1100 and OVSC1800). YES NO

Are auditors able to describe and demonstrate their responsibilities in accordance with USSID CR1610? YES NO

Are procedures in place to terminate a person's database access when such access is no longer required? YES NO

17. Does the unit task targets? YES NO

Are proper checks for foreignness conducted prior to tasking? YES NO

Are any checks for foreignness conducted thereafter? YES NO



18. Does the unit issue SIGINT reports or products?	YES	NO
Are proper sanitization or minimization procedures incorporated into pre-release quality control?	YES	NO
Are SIGINT reports reviewed after release for sanitization or minimization concerns?	YES	NO
19. Has the unit's intelligence oversight program for SIGINT been subjected to prior inspections or staff assistance visits? Has the unit conducted inspections of its own operations?	YES	NO
20. Has the unit developed or employed any intelligence oversight initiatives related to its SIGINT mission (For example, training tools, SOP, policy letters, or procedural guidelines)?	YES	NO
21. Do unit personnel understand the basic principles of intelligence oversight?		
Why intelligence oversight is important?	YES	NO
Why there a need for oversight in the intelligence community?	YES	NO
Why intelligence oversight is important for the Army?	YES	NO
What constitutes a U.S. person?	YES	NO
Who their SIGINT Intelligence Oversight officer is?	YES	NO
22. Do personnel engaging in SIGINT activities have access to the documents described in para 12, above?	YES	NO
23. Test the ability of unit personnel to define what types of incidents would constitute reportable matters.		
24. Do personnel understand the mechanics for submitting a Signals Intelligence related incident report, including the timelines for reporting?	YES	NO

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

1. Does the unit's mission involve the acquisition of publicly available information (para 1-5d, AR 381-10)?	YES	NO
2. Can the information be acquired without special legal authorizations, such as court orders, search warrants, or approval of special collection techniques or operational concepts?	YES	NO
3. If the unit is collecting U.S. person information, does it have a legitimate mission to collect this information and does collection comply with the requirements of Procedure 2, AR 381-10 (para 1-5d, AR 381-10)?	YES	NO
4. Has any requirement to disclose affiliation with the intelligence community been identified and addressed in accordance with Procedure 12?	YES	NO
5. Does the collection comply with obligations not to focus on a person solely because of race, ethnicity, national origin, religion, or the First Amendment rights of free speech and assembly (para 2-5, AR 381-10)?	YES	NO
6. Is the method of collection authorized and appropriate to the mission of the unit?	YES	NO
7. Is the information being retained and disseminated in accordance with Procedures 3 and 4, AR 381-10?	YES	NO
8. If the unit is engaging in collection from internet sources in which access to the public is meaningfully restricted, is this activity being accomplished by authority of an approved CISOC)(para 8-8c, AR 381-20)?	YES	NO
9. If the unit is using non- or mis-attributable internet access provided by a commercial internet service provider, has the authority to do so been properly documented in accordance with para 1-9b, AR 381-10 and DCS, G-2 Memo (S//NF), subject: Nonattributable Internet Access (U), dated 17 Dec 07?	YES	NO