

DEPARTMENT OF THE ARMY, DEPUTY CHIEF OF STAFF,

G-2

INTELLIGENCE OVERSIGHT

ASSESSMENT/INSPECTION GUIDE

APRIL 2015

ADMINISTRATIVE INFORMATION

Organization: _____

Date of Assessment: _____

Type of Assessment / Inspection: _____

Intelligence Oversight Officer (IOO)	
Alternate IOO	
Legal Advisor	
IOO for SIGINT (if applicable)	
Alternate IOO for SIGINT (if applicable)	
Contact Information	

Mission of Unit:

NOTE: According to Department of the Army guidelines, an inspector has three levels that he/she may use to categorize findings. They are failing deficiency (shortcomings that immediately cause a unit to fail the inspection), deficiency (multiple deficiencies can result in a failing grade), and observation (notes from the inspector to the unit to indicate areas in which the unit needs improvement). Checklist items highlighted present *potentially* failing deficiencies.

Recommendations for Inspected Program Administrators

- Immediately inform your chain of command of the visit. Your chain of command should not be surprised to see visitors in the unit.
- Ensure your program is well-advertised (smart cards, posters)
- Prepare unit personnel (ensure they can answer basic questions about the Intelligence Oversight Program (IOP) (define QIAs, RFCs, S/HSM; identify QIA reporting channels & deadlines; be able to navigate to references online; etc.)
- Post previous inspection results in your continuity binder. Have memoranda prepared addressing corrections for the deficiencies/observations noted in previous inspections.
- Be present. The primary IOO should be the primary host of the assessment/inspection. Do not delegate this responsibility to the Alternate.
- Prepare Command and Intelligence Oversight briefings. Brief should explain unit's mission, authorities, current operations, C2, Questionable Intelligence Activity (QIA) reporting methods, approved special collection techniques, status of QIA investigations, etc. Arrange interviews (Command IG, Command Judge Advocate (CJA)/Staff Judge Advocate (SJA), IOO for SIGINT, G2X, HOC Chief, ATCICA, OSINT, ACE personnel, etc...). Be prepared to discuss with unit leaders their commitment to intelligence oversight.
- Prepare unit training records for review.
- Set up the In-Brief –Mandatory (includes in brief by visiting group, command brief of unit being inspected, and overview of unit Intelligence Oversight Program (IOP).
- Set up the Out brief – Mandatory.
- Coordinate with unit CJA, SJA.
- Review past inspections or QIA investigations.
- Sensing sessions with a variety of individuals working in all disciplines.
- Have a good understanding about the organization's mission and authorities.
- Out brief the unit commander, or unit leaders (e.g. G2, Deputy G2)
- Draft evaluation report.

**INTERNAL AND EXTERNAL ASSESSMENTS/INSPECTIONS
(Includes inspections under the unit's OIP)**

	Yes	No	Comment
1. Is Intelligence Oversight included in the unit's OIP (para 1-4b(6), AR 381-10?			
1a. When was the last organizational Intelligence Oversight inspection.			
1b. Attach previous inspection report.			
1c. Were all deficiencies corrected?			
1d. Were corrective actions taken?			
1e. Assess the organization's relationship with the command IG.			
1f. When was the last external Intelligence Oversight inspection conducted? (External includes inspections by local command IG, DAIG, Department of Defense Intelligence Oversight Office.			

INTELLIGENCE OVERSIGHT OFFICERS

	Yes	No	Comment
2. Are primary IOOs appointed in writing (para 1-4p(4), AR 381-10?			
2a. Are Alternate IOOs appointed in writing (para 1-4p(4), AR 381-10?			
2b. Are they appointed on orders signed by the commander?			
2c. Are the ranks of the IOOs commensurate with their responsibilities and the size of the unit?			
2d. Have appointed IOOs completed the Intelligence Certification Course offered online?			
2e. Is the primary IOO an experienced intelligence professional and a member of the operational chain of command? (NOTE: THE IOO NEED NOT BE ASSIGNED TO THE G3/S3, BUT THE IOO DOES NEED TO BE IN A POSITION WHERE HE/SHE HAS ACCESS TO			

	Yes	No	Comment
<i>INFORMATION ON THE UNIT OR COMMAND'S INTELLIGENCE OPERATIONAL MISSION APPROVAL AND REPORTING PROCESS.)</i>			
2f. Are the IOOs' duties detailed in the appropriate personnel evaluation support form?			
2g. Does the IOO have unfettered access to procedures, programs, files, networks, databases, reporting and data necessary for the conduct of thorough and comprehensive oversight (paras 1-4h(7), 1-4i(6), 1-4k(6), 1-4m(6), and 1-4p(4), AR 381-10 (Unfettered access includes conducting reviews of OPORDs, FRAGOs, CIOPs, CISOCs, and any other operational proposal before execution.)?			
2h. Does the IOO have access to unit intelligence reporting and products prior to publication?			

INTELLIGENCE OVERSIGHT POLICY

	Yes	No	Comment
3. Does the unit maintain an Intelligence Oversight binder for his/her use (maintained either online or as a paper document)?			
3a. Are the following Intelligence Oversight essential documents available for inspection? (Hard or soft copy)			
3a(1). Executive Order 12333, United States Intelligence Activities, Dec 81			
3a(2). DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 82			
3a(3). Directive Type Memorandum 08-052, DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters, 17 Jun 09, (current version)			
3a(4). Army Regulation 381-10, US Army Intelligence Activities, 3 May 07			
3a(5). Unit policy memorandum/letter on Intelligence Oversight			
3a(6). Unit Intelligence Oversight SOP			
3b. Does the unit policy and SOP include contractors?			
3c. Does the IOO have an understanding of what are the governing policies?			

INTELLIGENCE OVERSIGHT TRAINING

	Yes	No	Comment
4. Does the organization have an Intelligence Oversight training program with personnel receiving both initial and refresher training? (para 14-1b, AR 381-10).			
4a. How are training records maintained? (e.g. DTMS)			
4b. How is training delivered?			
4c. Is training tailored to the unit's mission?			
4d. How is the effectiveness of the training evaluated?			
4e. Are incoming personnel receiving Intelligence Oversight training within 30 days of arrival (para 14-1b, AR 381-10)?			
4f. Are contractors receiving Intelligence Oversight training? (para 1-4p(3), AR 381-10)			
4g. How is the training documented?			
4h. ASCC Commanders typically do not have MI backgrounds. What is the level of Intelligence Oversight understanding among the ASCC leadership?			

TRAINING STATISTICS, AS A PERCENTAGE OF PERSONNEL ASSIGNED IN EACH CATEGORY

	Soldiers	Civilians	Contractors
First 30 days	Ex. 47/50 assigned (94%)		
Refresher Training			
Percent of the total			

REPORTING QUESTIONABLE INTELLIGENCE ACTIVITY AND REPORTABLE FEDERAL CRIMES

	Yes	No	Comment
5. Are internal procedures established to report QIA and reportable federal crimes (IAW AR 381-10)?			
5a. Do personnel understand what must be reported IAW Procedure 15 (para 15-4, AR 381-10)?			
5b. Are employees and supervisors reporting QIA and reportable federal crimes upon discovery (para 14-2c and 15-2a, AR 381-10)?			
5c. Are Procedure 15 and Chapter 16 reports sent to DAIG within five (5) working days of discovery (para 15-2b, AR 381-10)?			
5d. Are employees aware they can submit Procedure 15 reports directly to the DAIG, the Deputy Chief of Staff G2, the Army General Counsel, or other officials specified in para 15-2a, AR 381-10?			
5e. Is the command conducting inquiries of QIA, when appropriate (para 15-3, AR 381-10)?			
5f. What mitigation strategy (e.g. education, training, updated procedures, AR 15-6 findings) has the unit enacted to ensure that QIAs previously reported as Procedure 15 do not continue to be a problem?			
NOTE: INSPECTORS WILL ASSESS HOW THE UNIT HAS IMPLEMENTED CHANGES AND IMPROVEMENTS IN THE WAKE OF A QIA.			
5g. Are there indications that QIAs have not been reported as required?			
5h. Do personnel understand what must be reported IAW Chapter 16 (para 16-3 and 16-4, AR 381-10)?			
5i. Are Chapter 16 reports sent to DCS, G-2 within five (5) working days of discovery (para 16-2a-b, AR 381-10)?			

COLLECTION OF US PERSON INFORMATION

Authorized Categories for Collection of US Person Information

**Consensual
Publicly Available Information
Foreign Intelligence
Potential Sources of Assistance
Communications Security
Threats to Safety
Administrative Purposes**

**Protecting Intelligence Sources and Methods
Physical Security
Counterintelligence
Personnel Security
Narcotics
Overhead Reconnaissance**

	Yes	No	Comment
6. Does the mission of the organization involve the collection, retention, or dissemination of information on US Persons for intelligence purposes?			
Mission to Collect?			
Mission to Retain?			
Mission to Disseminate?			
6a. Is the unit collecting US Person information legitimately IAW its assigned mission and AR 381-10?			
6b. Does the unit's collection of US Person information meet one of the thirteen categories defined in para 2-2, AR 381-10?			
6c. Do IOOs and unit personnel understand that AR 381-10 does not itself authorize intelligence activity (para 1-5a, AR 381-10)?			
6d. If the unit collects US Person information as part of an assigned mission, what procedures are in place to ensure that such information is collected and retained IAW the mission and the policies of AR 381-10?			
6e. If the unit is disseminating US Person Personal Identifiable Information (PII), what is their mechanism to determine if the recipient is entitled to receive it?			

ANNUAL FILES REVIEW

	Yes	No	Comment
7. Does the unit conduct an annual review of intelligence files and databases in order to determine if retention of US Person information continues to be necessary to an authorized function of the unit (para 3-3c, AR 381-10)?			
7a. Does the unit review of all operational audio/video recording equipment (digital cameras, voice recorders, etc) to ensure data management is IAW handling US persons data.			
7b. What intelligence files and databases does the unit maintain that contain information about US Persons?			
7c. What method is used to conduct the annual files review?			
7d. How does the unit evaluate the effectiveness of the review?			
7e. Are reviews of databases conducted on a regular basis to ensure that US Person information has not been retained longer than may be authorized or necessary (para 3-3c, AR 381-10)?			
7f. Is there documentation when the last annual files review was conducted?			

SPECIAL COLLECTION TECHNIQUES

	Yes	No	Comment
8. Does the unit employ special collection techniques as specified in Procedure 5 through 10, AR 381-10?			
8a. Is the unit employing special collection techniques IAW its mission and authorities?			
8b. 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?			
8c. Have requests for the use of special collection techniques been reviewed and approved by proper legal authority?			
8d. 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)?			
8e. If a special collection technique has been authorized for a certain period of time, has the unit stayed within the limits of the order or counterintelligence special operations concept (CISOC)?			
NOTE: THE INSPECTOR SHOULD REVIEW DOCUMENTATION (OPORD, CISOC) 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.			
8f. Are the intelligence reports generated by the special collection technique reviewed by the IOO prior to publication?			
8g. Has the unit requested any Procedure 10s?			

USE OF BIOMETRIC EQUIPMENT

	Yes	No	Comment
9. Does the unit maintain or use biometric equipment?			
9a. If yes, does the unit have a copy of DCS G2			

Memorandum, Policy on Collection and Retention of Biometrics Data and Contextual Information in the United States by US Army Military Intelligence Personnel, 15 Jan 09?			
9b. Is the unit in possession of biometric devices including information on the permissible use of these devices in annual oversight training?			
9c. Are biometric devices in use in the US being employed only for training purposes or a properly authorized function?			
9d. Is biometric data gathered during training deleted at the end of each training session or redeployment?			

INTELLIGENCE SUPPORT TO FORCE PROTECTION

	Yes	No	Comment
10. Does the unit provide intelligence support to force protection?			
10a. If the organization is located in the US, is the collection of force protection information focused on data related to foreign intelligence and international terrorism (para 17-1b, AR 381-10)?			
10b. If MI elements providing support to force protection receive US 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?			
10c. Are intelligence organizations controlling or maintaining force protection data bases in the US in contravention of AR 381-10 (para 17-1g, AR 381-10)?			
10d. Is there a legitimate reason the unit intelligence section or officer is responsible for Force Protection rather than the unit operations officer or section? (assuming that this is so)			
NOTE: INSPECTORS SHOULD BE ABLE TO ASSESS THE RELATIONSHIP BETWEEN THE UNIT COMMANDER AND GARRISON PROVOST MARSHAL'S OFFICE.			

CHECKLIST TAILORED FOR UNITS WITH OPEN SOURCE INTELLIGENCE (OSINT) MISSIONS

	Yes	No	Comment
11. Does the unit have authorized mission, authority and purpose to conduct OSINT?			
11a. List each OSINT tool and its capability that the unit employs.			
11b. Are personnel properly trained on using the tool(s)?			
11c. Is OPSEC included in the training?			
11d. Does the unit have established procedures for the periodic review of all OSINT operations and report holdings to ensure compliance with policy and regulations?			
11e. Does the unit maintain a copy of the Army Directive for OSINT?			
11f. Is the use of OSINT consistent with applicable laws, regulations, and other Intelligence Oversight policies?			
11g. Is there any indication that personnel are using private computer systems in an off-duty capacity to fulfill intelligence requirements?			
11h. Is there any indication that personnel are accessing online sites requiring log-in and passwords to access them for an intelligence purpose?			
11i. Are unit contractors involved in OSINT activities?			
11j. Does the unit conduct activity other than OSINT that utilizes the Internet?			
11k. Does the IOO understand the difference between authorized and unauthorized OSINT activity?			
11l. How does the unit control US Person data when information is derived from OSINT? (Address this for retention and dissemination.)			

CHECKLIST TAILORED FOR UNITS WITH COUNTERINTELLIGENCE (CI) MISSIONS

	Yes	No	Comment
12. Does the unit have the authority and mission to conduct CI?			
12a. Does the unit have the authority to collect/acquire US Person information? If so, evaluate the unit's scope of authority using AR 381-20, Chapters 5 & 10.			
12b. Does the unit have the authority to investigate? If so, evaluate the unit's scope of authority using AR 381-20, Chap 4.			
12c. Does the unit have the authority to conduct operations? If so, evaluate the unit's scope of authority using AR 381-20, Chap 10.			
12d. Does the unit have the authority to conduct analysis and production? If so, evaluate the unit's scope of authority using AR 381-20, Chap 6.			
12e. Does the unit conduct CI support to technology and critical infrastructure? If so, evaluate the unit's scope of authority using AR 381-20, Chap 7.			
12f. Does the unit conduct CI support to Cyber? If so, evaluate the unit's scope and authority using AR 381-20, Chap 8.			
12g. Does the unit conduct CI support to Force Protection? If so, evaluate the unit's scope and authority using AR 381-20, Chap 9.			
12h. Does the unit have a polygraph and credibility assessment program mission? If so, evaluate the unit's scope and authority using AR 381-20, Chap 11.			
12i. Does the unit provide CI support to the Combatant Commanders? If so, evaluate the unit's scope and authority using AR 381-20, Chap 12.			
12j. Does the unit provide other CI support-related functions and involved in other technical activities? If so, evaluate the unit's scope and authority as it relates to their other missions using AR 381-20, Chap 13 & 14.			
12k. Evaluate the unit's Insider Threat Program (AR 381-12 and AR 381-20, Chap 16).			

	Yes	No	Comment
12l. Do CI personnel assigned to the unit carry badge and credentials (B&C)? If so, briefly assess the unit's B&C inspection program and explain Intelligence Oversight concerns involving misuse of B&Cs.			
12m. Are all CI activities properly coordinated with the ACICA/ATCICA?			
12n. Identify all the databases and systems the unit utilizes to conduct its mission.			
12o. Does the unit have the following CI related policy documents readily available for use by persons engaging in CI investigations or operational activities?			
12o(1). Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (Delimitations Agreement), 1979			
12o(2). Supplement to 1979 FBI/DoD Memorandum of Understanding, Coordination of Counterintelligence Matters, 1 Apr 96			
12o(3). Memorandum of Understanding Between the FBI and DoD Governing Information Sharing, Operational Coordination, and Investigative Responsibilities, 2 Aug 11			
12o(4). 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			
12o(5). Annex B, Counterintelligence Information Sharing,			

	Yes	No	Comment
to the Memorandum of Understanding Between the FBI and DoD Governing Information Sharing, Operational Coordination, and Investigative Responsibilities, 9 Dec 11			
12o(6). AR 381-12, Threat Awareness and Reporting Program (TARP), 4 Oct 10			
12o(7). AR 381-14 (C), Technical Counterintelligence (U), 30 Sep 02 (if appropriate)			
12o(8). AR 381-20 (S//NF), The Army Counterintelligence Program (U), 25 May 10			
12o(9). 381-47 (S//NF), Offensive Counterintelligence Operations (U), 17 Apr 06			
12o(10). AR 381-141 (C), Intelligence Contingency Funds (ICF)(U), 16 Jan 04 (if appropriate)			
12p. Do unit personnel understand CI investigative jurisdiction in both CONUS and OCONUS and do personnel know where to go for answers if they have questions (paras 4-3 and 4-4, AR 381-20 and the Delimitations Agreement)?			
<i>NOTE: DOES THE 2X PROVIDE NECESSARY GUIDANCE TO SUPPORTED COMMANDERS BY ADVISING HOW CI SUPPORTS USING TACTICS AND TECHNIQUES IAW APPLICABLE POLICY, DOCTRINE, AND LAW?</i>			

CHECKLIST TAILORED FOR UNITS WITH A HUMAN INTELLIGENCE (HUMINT) MISSION

	Yes	No	Comment
13. Does the unit have established procedures for the periodic review of all HUMINT operations to ensure compliance with policy and regulations?			
13a. Are operational proposals (OP) submitted for review and approval by proper authority before any HUMINT activity is conducted?			
13b. Are approved Ops current?			
13c. Are all Army HUMINT activities coordinated with INSCOM G2X and/or Army G2X?			
13d. Is collection of US Person information done IAW the provisions of AR 381-10?			
13e. Is the unit conducting FORMICA?			
13f. If so, under whose authorities?			
13g. Does the unit provide live environment training?			
13h. If so, how is Intelligence Oversight included in the training?			
13i. Do HUMINT collectors and support personnel understand what constitutes an Intelligence Oversight reportable incident and how to report it?			
13j. Does the unit have the following documents readily available for use by persons conducting HUMINT activities?			
13j(1). DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect US Persons, Dec 82			
13j(2). DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, Incorporating Change 1, 15 Nov 13			
13j(3). DoDD S-5200.37, Management and Execution of Defense Human Intelligence (U), Incorporating Change 2, 18			

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	Yes	No	Comment
Nov 13			
13j(4). DoDI S-5200.42, Defense Human Intelligence (HUMINT) and Related Intelligence Activities (U), Incorporating Change 2, 16 Oct 13			
13j(5). DoDI S-5205.01, DoD Foreign Military Intelligence Collection Activities (FORMICA) (U), 9 Mar 15			
13j(6). DoDI S-3325.07, Guidance for the Conduct of DoD Human Source Validation (U), 22 Jun 09			
13j(7). DoDD S-3325.09 - Defense Clandestine Source Operations (Ch 2), 15 Jul 14			
13j(8). DoDI S-3325.10 - HUMINT Activities in Cyberspace - 6 Jun 13			
13j(9). AR 381-10, US Army Intelligence Activities, 3 May 07			
13j(10). AR 381-100 (S), Army Human Intelligence Collection Programs (U), 15 May 88			
13j(11). DCS, G-2 Memo (S//NF), Interim Policy Guidance for the Conduct of Oversight of Army Human Intelligence (HUMINT) Source Operations (U), 13 Jun 11			
13j(12). AR 381-102 (S), US Army Cover Support Program (U), 10 Jan 91			
13j(13). AR 381-141 (C), Intelligence Contingency Funds (ICF) (U), 16 Jan 04			
13j(14). DHE-M Vol.I 3301.001 (S//NF), Collection Requirements, Reporting, and Evaluation Procedures (U), Incorporating Change 2, 1 Feb 12			
13j(15). DHE-M Vol. II 3301.002 (S//NF), Collection Operations (U), 23 Nov 10			
13j(16). DA Pam 381-15 (S//NF), Foreign Military intelligence Collection Activities Program (U), 8 Aug 13			
13j(17). FM 2-22.3 (U), Human Intelligence Collector Operations, 6 Sep 06			
<i>NOTE: DOES THE 2X PROVIDE NECESSARY GUIDANCE TO SUPPORTED COMMANDERS BY ADVISING HOW CI SUPPORTS USING TACTICS AND TECHNIQUES IAW APPLICABLE POLICY, DOCTRINE, AND LAW?</i>			

CHECKLIST TAILORED FOR UNITS WITH A SIGNALS INTELLIGENCE (SIGINT) MISSION

	Yes	No	Comment
14. What is the source of the unit's authority to engage in a SIGINT mission?			
14a. Does the unit provide SIGINT personnel to perform duty with an NSA element?			
14b. Does the unit conduct a national SIGINT mission delegated by an NSA element?			
14c. Does the unit conduct an Army SIGINT mission, as approved by DIRNSA, under delegated SIGINT Operational Tasking Authority (SOTA)?			
IF ANSWERS TO THE LAST TWO QUESTIONS ARE NO, SKIP TO QUESTION 14z.			
14d. If the unit is currently conducting a SIGINT mission, is its authority to do so specified in valid authority documentation on file (USSID/Site Profile, Mission Delegation Form (MDF), and Staff Processing Form (SPF))?			
14e. Are the unit's entries in NSA SIGINT Address Book (SAB) and Goldpoint database correct?			
14f. Is the unit commander and G2/S2 knowledgeable of and fulfilling their Intelligence Oversight responsibilities IAW USSID SE1000, Annex A (Intelligence Oversight for Army Signals Intelligence (SIGINT) Operations)?			
14g. Are the commander and other senior leaders included in SIGINT Intelligence Oversight awareness training provided by the SIGINT Oversight Officer (SIOO)?			
14h. Does the organization have a primary and alternate Intelligence Oversight Officer for SIGINT operations (USSID SE1000, Annex A)?			
14i. Are the SIOOs actively involved in unit's SIGINT mission?			
14j. Are primary and alternate SIOOs appointed on orders signed by the commander?			
14k. Are SIOOs knowledgeable of and fulfilling their responsibilities as directed in USSID SE1000, Annex A?			
14l. If able to access an NSANet or JWICs workstation,			

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	Yes	No	Comment
have SIOOs completed OVSC2201 (Intelligence Oversight Officer) training? (Note: This requirement is in addition to OVSC1000 (NSA/CSS Intelligence Oversight Training), OVSC1100 (Oversight of Signals Intelligence Authorities), and OVSC1800 (Legal Compliance and Minimization Procedures) courses that are required for everyone.)			
14m. Where practical, is there a SIOO present at all locations where the unit is engaging in a SIGINT mission?			
14m(1). In locations where a SIOO is not present, has the parent organization provided adequate Intelligence Oversight training and oversight?			
14m(2). Does the SIOO interface regularly with the SIGINT elements?			
14n. Does the SIOO maintain a continuity book, to keep and show required documentation and aid in transitions from outgoing to incoming SIOOs?			
14o. If the unit is currently conducting a SIGINT mission, has it submitted an IOO Verification Form or accepted the Intelligence Oversight lien in GATEKEEPER, via Army Cryptologic Operations (ACO) to the NSA/CSS SID Oversight and Compliance Office (SV)?			
14p. Has the unit submitted any SIGINT related incident reports in the past year?			
14p(1). If yes, were the reports submitted within 72 hours of discovery?			
14p(2). Was the commander aware of these reports and was he/she involved in mitigation procedures?			
14p(3). Was a summary of the incident(s) included in the Quarterly Intelligence Oversight Report?			
14p(4). Has the unit failed to report any SIGINT related Intelligence Oversight matters?			
14q. Has the unit submitted quarterly Intelligence Oversight reports to ACO (and any other required offices)?			
14q(1). Were these reports submitted on the first duty day			

	Yes	No	Comment
following the end of the quarter?			
14q(2). Were the reports signed by unit leadership (commander, S2, or ACE Chief)?			
14q(3). Does the SIOO brief the contents of reports to unit leadership prior to submitting them to ensure their complete knowledge of the event?			
14q(4). Does the unit maintain copies of signed reports on file for at least three (3) years?			
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.			
14r. If the unit has a Sensitive Compartmented Information Facility (SCIF), do SIGINT personnel 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.)			
14r(1). USSID SE1000 (US Army Cryptologic Forces – SIGINT Activities), 24 Oct 13 (U) (or most recent update)			
14r(2). USSID SE1000, Annex A (Intelligence Oversight for Army Signals Intelligence (SIGINT) Operations), 10 Apr 13 (U//FOUO)			
14r(3). USSID SE1200 (US Army Cryptologic Forces – Expeditionary SIGINT Activities), 15 Aug 12 (U) (or other appropriate overarching USSID)			
14r(4). USSID SP0018 (Legal Compliance and US Persons Minimization Procedures) (U//FOUO), 25 Jan 11			
14r(5). USSID SP0019 (NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy) (U//FOUO), 13 Nov 12			
14r(6). DCS, G-2 Memo, Interim Policy for Intelligence Oversight of Army Signals Intelligence (SIGINT) Operations, 29 Oct 10			
14r(7). NSA/CSS Policy 1-23 (Procedures Governing NSA/CSS Activities that Affect US Persons), 30 Jul 13 and			

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	Yes	No	Comment
classified Annex to DoD 5240.1-R, 16 Sep 11			
14r(8). Identities in SIGINT Manual, 11 May 12			
14r(9). National Security Council Intelligence Directive (NSCID) Number 6, 17 Feb 72			
14r(10). Presidential Policy Direction (PDD)-28, (Signals Intelligence Activities), 17 Jan 14			
14s. 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?			
14s(1). OVSC1000, NSA/CSS Intelligence Oversight Training			
14s(2). OVSC1100, Oversight of Signals Intelligence Authorities			
14s(3). OVSC1800, Legal Compliance and Minimization Procedures			
14t. Do authorized personnel currently access raw SIGINT databases?			
14t(1). If required, are qualified primary and alternate auditors assigned and available?			
14t(2). Have auditors received OVSC3101 on-line training (this is in addition to OVSC1000, OVSC1100, and OVSC1800)?			
14t(3). Are auditors able to describe and demonstrate their responsibilities IAW USSID CR1610?			
14t(4). Are procedures in place to terminate a person's database access when such access is no longer required?			
14u. Does the unit task targets?			
14u(1). Are proper checks for foreignness conducted prior to tasking?			
14u(2). Are any checks for foreignness conducted thereafter?			
14v. Does the unit issue SIGINT reports or products?			
14v(1). Are proper sanitization or minimization procedures incorporated into pre-release quality control?			

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	Yes	No	Comment
14v(2). Are SIGINT reports reviewed after release for sanitization or minimization concerns?			
14w. Has the unit's Intelligence Oversight Program for SIGINT been subjected to prior inspections or staff assistance visits?			
14x. Has the unit conducted inspections of its own operations?			
14y. Has the unit developed or employed any Intelligence Oversight initiatives related to its SIGINT mission (training tools, SOP, policy, or procedural guidelines)?			
14z. Have all personnel received required 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)?			
14aa. Do unit personnel understand the basic principles of Intelligence Oversight?			
14aa(1). Why is there a need for oversight in the Intelligence Community?			
14aa(2). Who are US Persons?			
14aa(3). Who is your unit SIOO?			
14aa(4). While conducting SIGINT, what types of incidents would constitute a reportable incident?			
14aa(5). What is the procedure/process for submitting a SIGINT-related incident report?			