DoD SIOO Intelligence Oversight
Inspection Guide

UNIT:_____   Date:_____   Inspectors:_____

General Program Organization

1. Are unit personnel aware of and do they understand the unit's authorized intelligence mission set?   YES   NO

2. What is the authorized mission?

3. Has the organization designated an individual with overall responsibility for the IO program?   YES   NO
        -Are duties delineated?   YES   NO
        -Are duties reflected in appropriate Support Form?   YES   NO
         - Does he/she have access to all intelligence and intelligence related programs, files
            networks, and information for operations or activities conducted by the organization?   YES   NO
        - Is there anyone else who has some IO responsibility such as the unit SJA   YES   NO

4. Review IO Officer/NCO files. Does the unit have an IO Policy Book (brigade/group level),   YES   NO
     Local IO resources, or access via the internet to the following references?

     -Executive Order 12333, United States Intelligence Activities, December 1981 as amended (July 08)
     -DOD Directive 5240.01, DoD Intelligence Activities, 27 August 2007.
     -DOD Directive 5240.1-R, Procedures Governing the Activities of DOD Intelligence Components
         That Affect United States Persons, December 1982.
     -DTM 08-052, DoD Guidance for Reporting Questionable Intelligence Activities
         and Significant or Highly Sensitive Matters," June 17, 2009 [with Change 3 of July 30, 2012]
     -Service or Agency Regulations and Policy Documents.
     -Unit specific/unique documents (e.g. OPORDS, memorandum, etc.) governing the unit's missions
         and/or activities
     -Unit IO SOP (not required by regulation but a good practice)
     -DoD SIOO Intelligence Oversight Training and Resource Disk (March 2011)

5. Other than appropriate administrative files, as required, do any files (automated, operational,   YES   NO
working, etc.) contain information about US persons? If "**YES**," confirm the organization's
authority to collect, retain, and disseminate such US person information and review authorization
documentation for currency.

Training

6. Do personnel receive Intelligence Oversight training?   YES   NO
        -What is the frequency required by the organization?
        -What percentage of assigned personnel are documented as current for training?
        -What is the method of delivery: (Online, group platform instruction, deskside)
        -Is unit leadership made aware of IO requirements? How?   YES   NO
        -Does unit leadership participate in IO training?   YES   NO
        -Is training tailored to the unit's mission and adequate in content?
        -Is training effectiveness evaluated?   YES   NO
        -Is training documented and are records current?   YES   NO
          YES   NO

-Are new unit personnel briefed as part of in- processing?	YES	NO
-Is there a requirement for IO refresher training? Frequency?	YES	NO
-Are contractors required to **take** training?	YES	NO
-Are measures in effect to ensure personnel absent during scheduled training receive	YES	NO
IO training? Describe how this is done and cross check training records.		
-Are any personnel in the unit exempted from IO training?	YES	NO
What is the basis for the exemption?		

Who made the decision?

Has service or agency IG been notified?	YES	NO
-Is an Intelligence Oversight reference guide/smart card provided to personnel?	YES	NO
Review content for accuracy and adequacy.		

7. Based on personnel interviews, are organization personnel aware of:
-What constitutes a U.S. person?
-What constitutes a questionable intelligence activity?
-What obligation personnel have to report questionable intelligence activities?
-To whom personnel report questionable intelligence activities?
-The fact that no retaliatory action can be taken for reporting questionable intelligence activities?
-Where to find applicable directives, regulations, and policies?
-The additional reporting requirements for QIAs and Significant or Highly Sensitive
     Matters IAW DTM 08-052?

8. How is the IO program advertised in the organization?

9. Are there any Information Operations staffs assigned to the inspected command/organization?

-If so, have they received IO training? Per para 3.1 of DoDD 3600.01	YES	NO
-Was the training tailored to address potential conflicts between intelligence and	YES	NO
informational operations per Encl 2, Para 10.h. of DoDD 3600.01.		

Oversight Mechanisms

***Internal Oversight**

10. Does the organization conduct internal self-assessments or inspections of the IO program?	YES	NO

What is the frequency?
How are assessments documented?

11. Are file review and verification procedures established IAW agency or service regulation?	YES	NO
Is the current files verification certificate on file?	YES	NO

How is the annual files verification reported to higher headquarters?

12. Are IO concerns effectively considered in unit operational planning and conduct?	YES	NO

How is this accomplished?
Who participates in the process?
What actions are taken to resolve concerns prior to plans being approved and
     operations executed?

13. Does the unit's mission allow, and is the unit conducting, intelligence operational activities requiring the use of special collection techniques (Procedures 5 through 10)?   YES   NO

        If "**YES**,"--Have all requests for the use of special collection techniques been reviewed   YES   NO
            by proper legal authority and approved by the appropriate command authority?
            (Review approval requests and approval documentation.)
        Were operators appropriately aware, prebriefed, monitored, and debriefed for each situation?   YES   NO
        Are records maintained on who was briefed and when?   YES   NO
        Are resulting reports/information executed/handled/disseminated/stored properly and correctly?   YES   NO

14. Have organization personnel conducted any undisclosed participation in domestic organizations for intelligence purposes or in support of intelligence activities?   YES   NO
        Was such participation approved by appropriate authority and documented?   YES   NO

15. Has the unit provided support to law enforcement agencies (LEA) since the last IO inspection?   YES   NO

        If **"YES,"** did the requests receive a legal review and were they approved by the   YES   NO
            appropriate command authority? (Review approval documentation.)

16. Has the unit conducted any intelligence or intelligence-related training that was executed to provide incidental support to civil authorities (a.k.a. Leveraging Military Training)?   YES   NO

        If "**YES,**" how were those activities planned and executed to ensure compliance with
            DoD 5240.1-R and applicable Service/Agency Intelligence Oversight?

17. Has the organization **collected** imagery of US persons or organizations located in CONUS?   YES   NO
    Has the organization **collected** image**r**y of US persons located outside CONUS?   YES   NO

        If **"YES,"** did the requests receive a legal review and were they approved by the   YES   NO
            appropriate command authority? (Review approval documentation.)

18. Does the unit participate in any intelligence SAP's or other restricted access programs?   YES   NO

        If **"YES,"**

        -What mechanisms are in place to ensure IO training of personnel and reporting
            Questionable Intelligence Activities involving the SAP?

        -What access does the command legal office and Inspector General have to provide
            oversight?

19. Are IIR's reviewed by the organization prior to publication?   YES   NO
    -Do IIRs containing US person information receive any special or additional review?   YES   NO

20. Does the organization have documented internal policies and procedures concerning collection, retention, and dissemination of US person information?   YES   NO
    -Are personnel aware of these policies and procedures and able to identify their reporting/approval chain?   YES   NO

21. What procedures exist to monitor the status of US person information held under the 90 day determination rule?

*Independent Oversight

22. Has IO been incorporated into the unit's Organizational Inspection Program (OIP)?   YES   NO

Date of last IO OIP _____

Were there any findings/observations? If "**YES**," review report.	YES	NO
Were corrective actions taken?	YES	NO

23. What external Intelligence Oversight inspections has the organization undergone since the previous   YES   NO
inspection by the current inspecting headquarters.

Date:_____   Inspecting Organization_____
Date:_____   Inspecting Organization_____
Date:_____   Inspecting Organization_____
Date:_____   Inspecting Organization_____
 (Review the reports of inspection.)

24. For any IO inspection listed in #22, above, in which there were findings/observations,
were corrective actions taken on findings/observations? Provide comments as applicable.   YES   NO

*Legal Oversight

25. What legal office provides advice and legal review of intelligence activities for IO equities?

26. What is the involvement of the organization's SJA or General Counsel in the oversight program?

Reporting Procedures

27. What internal periodic reporting requirements has the organization established?

28. Are required reports submitted in a timely manner as established by organization policy?   YES   NO

29. Are procedures established, and documented, to report questionable intelligence activities (QIA),   YES   NO
        Significant or Highly Sensitive Matters (S/HS) and Federal criminal activities to organization
        leadership within the timelines outlined in DOD 5240.1-R and DTM 08-052?

                What is the documented reporting process?
                (Crosswalk information from personnel interviews with the documented process.)

30. Review derogatory information in S-2 files for information reportable under Procedure 15 or
        as a Federal crime. Direct the unit to report if reportable information is found.

31. Has the unit reported any questionable intelligence activities under Procedure 15?   YES   NO
        (Review documentation.)

32. Are employees aware that DoDIG maintains a whistleblower protection program in the   YES   NO
        Department of Defense that encourages personnel to report fraud, waste, abuse and reprisal
        in accordance with DoDD 5106.01 and provides hotline links as avenues for such reporting?

33. Are employees aware of the following Hotline links and are they available on organization   YES   NO
        websites?

        NIPRnet   http://www.dodig.mil/Hotline/filing_info.html
        SIPRnet   http://www.dodig.smil.mil/hotline
        JWICCS   http://www.dodig.ic.gov/hotline/index.html

Response Mechanism

34. Does organization leadership understand it responsibilities to report QIAs to DoD SIOO?   YES   NO

35. Does organization leadership understand its responsibilities to ensure appropriate inquiry into reported QIAs and take appropriate corrective action based on a determination of the facts?   YES   NO

Information Sharing Environment

36. In the course of its official business does the organization/component/unit share or receive information with/from other Federal, State, Local or Tribal organizations, either intelligence organizations or non-intelligence organizations?   YES   NO

37. Does the organization/component/unit have a current list of major policy issuances in its IO Policy Book, including but not limited to the following?   YES   NO

   Executive Order 13356 – Strengthening the Sharing of Terrorism Information to Protect Americans
   ICD 501 – Discovery and Dissemination or Retrieval of Information within the Intelligence Community
   DoD Directive 5400.11 – DoD Privacy Program
   DoD Instruction 2000.26 – Suspicious Activity Reporting
   FBI/DOD MOU Governing Information Sharing, Operational Coordination, and Investigative Responsibilities

38. What procedures exist to verify that the requester has the appropriate clearances and a need to know?

39. What is the process for marking or tagging US Person information received from other organizations?

40. How is shared information that is being considered for permanent retention tracked?

41. Are there any requirements on how the receiving agency stores the information?

42. Are there any requirements governing the ability of the receiving agency to further share the information with other individuals or organizations?

43. What steps/procedures are in place to protect the USP information from unauthorized disclosure?

44. Are the organization's/component's/unit's information sharing procedures and/or requirements documented?

45. Has the organization/component/unit shared Suspicious Person Reports using the e-Guardian System?

46. Have the organization's/component's/unit's personnel completed Privacy and Civil Liberties training?

FOR CI UNITS ONLY

1. Does the organization have established procedures for review of all CI operations and investigations YES NO
to ensure compliance with DoD and service regulations?

2. Does the organization periodically review long-term CI special operations and investigations to YES NO
ensure continued regulatory compliance after initial approval?

3. Has the organization established procedures to ensure CISOCs, CIOCS, and threat assessments YES NO
receive legal and oversight reviews and are approved by the proper authority prior to implementation

4. Is release of information on US persons in accordance with the provisions of Procedure 4, YES NO
 DOD 5240.1-R?

5. Does the organization have available or access via internet to the following documents? YES NO

    DoD Directive 5240.02, December 20, 2007, Counterintelligence - Incorporating Change 1 December 30, 2010
    DoD Directive 5525.5, DoD Cooperation with Civilian Law Enforcement, 15 Jan 1986 - Incorporating Change 1
    December 20, 1989]
    DoD Instruction S-5240.09, October 29, 2008, Offensive Counterintelligence Operations (OFCO) (U)
    DoD Instruction 5240.04, February 2, 2009, Counterintelligence (CI) Investigations
    DoD Instruction 5240.05, February 22, 2006, Technical Surveillance Countermeasures (TSCM) Program
    DoD Directive 5240.06, May 17, 2011, Counterintelligence (CI) Awareness and Reporting
    DoD Instruction C5240.08, February 28, 2011 Counterintelligence Security Classification Guide
    DoD Instruction 5240.10, October 5, 2011, Counterintelligence Support to the Combatant
       Commands and the Defense Agencies
    DoD Instruction 5240.16, May 21, 2005, DoD Counterintelligence Functional Services
    DoD Instruction S5240.17, January 12, 2009, Counterintelligence Collection
    DoD Instruction 5240.18, November 17, 2009, Counterintelligence (CI) Analysis and Production
    DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program, August 27, 2007
    Incorporating Change 1, December 28, 2010
    DoD Instruction 5240.22, September 24, 2009, Counterintelligence Support to Force
     1979 FBI MOU Agreement Governing the Conduct of Defense Department Counterintelligence Activities
     in Conjunction with the Federal Bureau of Investigation, 5 Apr 1979
  1996 supplement to 1979 FBI MOU Regarding Coordination of Counterintelligence Matters, 1 Apr 1996
     Service and Agency Regulations and Instructions as Appropriate to Support Unit Mission
Service or Agency Policy Documents or Regulations

FOR HUMINT UNITS ONLY

1. Does the organization have established procedures for review of all HUMINT operations to ensure compliance with regulatory requirements, and DIAMs 3301.002 and DHM31301.002?   YES   NO

2. Does the organization periodically review long-term HUMINT operations to ensure continued compliance with DIAM 3301.002? (do they still have a valid mission authority?)   YES   NO

3. Has the organization established procedures to ensure OVOPs receive legal and oversight reviews and are approved by the proper authority prior to implementation?   YES   NO

4. Is release of information on US persons in accordance with the provisions of Procedure 4, DOD 5240.1-R?   YES   NO

5. Does the organization have available the following documentation as required by mission?   YES   NO

   DoD Directive-S 5200.37 "Management and Execution of Defense HUMINT," 29 May 2011
   DoD Instruction-S3325.07, "Source Validation," 16 August 2010
   DoD Instruction-C-5205.01, "DoD Foreign Military Intelligence Collection Activities (FORMICA),"
        January 22, 2009
   DoD Instruction-C-5200.42, "Defense Human Intelligence (HUMINT) and Related Intelligence Activities,"
        December 8, 2009
   DoD Instruction-S.5105.61, "Implementation of DoD Cover and Cover Support Activities," March 9, 1999
   Defense HUMINT Manual 3301.002, Defense Human Intelligence (HUMINT) Enterprise Manual,
   Volume II: Collection Operations, 23 November 2010
   Defense HUMINT Manual 3301.001, Defense Intelligence Agency Human Intelligence (HUMINT) Manual,
   Volume I: Collection Requirements, Reporting, and Evaluation Procedures, 30 January 2009
   Intelligence Community Directive #304, Human Intelligence," March 6, 2008, Amended 9 July 2009
   DoD/CIA Memorandum Of Agreement, "Operational Activities," July 2005
   Service or Agency Policy Documents and Regulations

FOR SIGINT UNITS ONLY   **(note: inspect from top down, CDR to IO Officer, to branch chiefs to operators)**

1. What is (are) the organization mission(s) (Unit USSID/Profile, Mission Delegation Form(s) Staff Processing Form(s)? When were they last updated and reviewed by the Service Cryptologic Element?

2. Does the organization have available in hard copy or online access to the current copies   YES   NO
of the following documents?

         -Executive Order 12333   YES   NO
         -DoD Directive 5240.1-R Procedures 1-4 and 14-15   YES   NO
         -NSA/CSS Policy 1-23   YES   NO
         -USSID SP0018   YES   NO
         -NSCID 6   YES   NO

3. Have all personnel received annual training on the requirements and restrictions of:

         -Executive Order 12333   YES   NO
         -DoD Directive 5240.1-R Procedures 1-4 and 14-15   YES   NO
         -NSA/CSS Policy 1-23   YES   NO

4. Have all personnel participating in SIGINT operations received annual training on the
 requirements and restrictions of USSID SP0018?   YES   NO

5. Do personnel know what constitutes a USSID SP0018 violation?   YES   NO

6. Do personnel know the procedures if uncertain a USSID SP0018 violation occurred?   YES   NO

7. Do personnel know the procedures for reporting a USSID SP0018 violation?   YES   NO

8. Has the unit reported a USSID SP0018 violation within the last year?   YES   NO

If "NO" go to 10

9. Describe the USSID SP0018 violations(s) that occurred and what transpired.

10. Do personnel access raw SIGINT databases?   YES   NO

 If "NO" go to 17

11. Have all personnel accessing databases **completed online training**   YES   NO
within the time requirements mandated by NSA?

12. Do personnel have access to Protect America Act (PAA) or FISA Amendment**s** Act (FAA) data?   YES   NO

If "NO" go to 14

13. Have all personnel accessing PAA/FAA data successfully completed the required training within   YES   NO
the time requirements mandated by NSA?

14. What raw SIGINT databases are accessed by assigned personnel. (Note: Response may be classified)

15. Is there a mechanism in place to track the reviewers (primary and secondary) for personnel   YES   NO
accessing raw SIGINT databases?

Check the following using the list of primary and secondary reviewers (representative sample):

  a. Reviewers (primary and secondary) are available to conduct reviews YES NO
    (not reassigned, TDY, etc.)

  b. Reviewers (primary and secondary) know that they are reviewers. YES NO

  c. Reviewers (primary and secondary) know their responsibilities YES NO

  d. Reviewers (primary and secondary) are qualified to be reviewers YES NO
  Observe auditors performing their auditing duties.

  e. Reviewers (primary and secondary) conduct reviews YES NO

  f. Review files are retained YES NO

16. Is there a mechanism in place to terminate a person's database access when access
is no longer required? YES NO

 If "YES" describe.

17. Does the unit task targets? YES NO

If "NO" go to 21

18. Is IO incorporated in target tasking procedures? YES NO

If "YES" describe.

19. Does the organization have any targets tasked requiring authorizations? YES NO

If "NO" go to 21

20. How does the organization manage tasked targets requiring authorizations (describe)?

21. Does the organization issue reports (serialized, time sensitive, summaries, etc.) YES NO

If "NO" go to 24

22. Is IO incorporated into the pre-release quality control for reports? YES NO

23. Are reports reviewed, post release, for IO concerns? YES NO

24.   Who in the organization submits quarterly reporting to NSA/OIG YES NO
(ask to see last two reports)

25. Is there a separate SIGINT IO officer? YES NO

26. Did he/she take the required online training? YES NO

2**7**. What are the mechanics for reporting incidents?

2**8**. Are they codified in a policy letter or SOP? YES NO