**A Practical Guide to Conducting Intelligence Oversight Inspections**

Inspections Instructor, SAIG-TR, 703-805-3895 DSN: 655

[usarmy.belvoir.usaignet.mbx.tigs-instructors@mail.mil](mailto:Graham.m.stone.mil@mail.mil)

Since an Inspector General’s primary method of providing oversight to his or her command’s Intelligence Oversight (IO) program is through an inspection, instruction at the U.S. Army Inspector General School (TIGS) only introduces IGs to IO as a concept and methodology. Students refer to The Intelligence Oversight Guide for more details and examples of the physical outputs emerging from the Preparation Phase of the Inspections Process. Given that these examples focus on the Military Intelligence companies within a division, field IGs often request further details of what an IO inspection entails in other types of units. This article provides greater fidelity to the inspection methodology for conducting an IO inspection on a non-military intelligence unit.

One of the enabling learning objectives for the IO block of instruction is to describe the recommended inspection methodology used by IGs to conduct Intelligence Oversight inspections as part of their command’s OIP. This methodology’s specific steps are:

1. Identify your command’s intelligence components.
2. Involve your local Staff Judge Advocate (specifically the Operational Law Attorney).
3. Request a briefing from these intelligence components on their intelligence oversight program’s compliance with AR 381-10.
4. Review their copy of AR 381-10 and appropriate SOPs.
5. Examine training records to determine if personnel are receiving training on AR 381-10.
6. Quiz unit or activity members on AR 381-10 using a test and scenarios.
7. Review unit procedures for handling all intelligence information.
8. Physically check the intelligence files for U.S. person information.
9. Check the unit or activity’s annual review of intelligence files, paying particular attention to support given to law-enforcement activities.
10. Determine if the unit or activity knows about Procedure 15 and how to report a questionable activity.

These steps provide the basis for a Detailed Inspection Plan on IO. My conduct of several IO inspections as the Chief of Inspections at an Army corps provide the basis for comments and suggestions made throughout this article. This article also includes lessons learned from an IO inspection from the Office of the Assistant to the Secretary of Defense on Intelligence Oversight (ATSD-IO) and a Staff Assistance Visit from the Forces Command (FORSCOM) IG office. Since steps 1 through 4 above are self-explanatory, I will focus on steps 5 through 10 above.

The typical IO training package and training records (Step 5) that I reviewed consisted of a slide packet of definitions followed by a sign-in roster indicating that the individuals had reviewed the training, a procedure used for both initial and annual training. The best training programs, however, have been scenario-based discussions tailored for the typical missions the unit will encounter. Good examples of scenarios are requests from within the command, in a garrison environment, to provide unmanned aerial vehicle (UAV) coverage over a field site for force-protection training or requests for sustainment training on biometric equipment. There are a myriad of ways either training could violate AR 381-10. Working through the controls to mitigate the chance of a potential violation is invaluable, not just to the military intelligence professionals but also to the command. For this reason, the best training programs also include the brigade and battalion leadership, specifically the commander, sergeant major, and operations officer. While these scenarios are useful for training, one may also use them as part of an evaluation to determine how much the command or military intelligence professionals know about IO.

In my inspections, I used both a closed-book quiz and scenario-based discussions (Step 6). I administered the closed-book quiz and then had the Soldiers exchange papers for grading. As we went through the answers for the quiz, we discussed the correct (and some of the incorrect) answers as discussion and teaching points. I then read and discussed several scenarios (some are included in The Intelligence Oversight Guide), which allowed me to assess further the unit’s knowledge of IO and to discuss teaching points. Using both of these methods allowed me to determine if attendees understood IO, what constitutes a questionable activity, and how to report it in accordance with Procedure 15 and local policy (Step 10). In my experience, most Soldiers (both officers and enlisted) failed the quiz and had a very limited understanding of IO. Typically, this method of inspection was the first time the unit had any scenario-based training on IO. Both methods of inspection also required initial preparation on the IG’s part to ensure that the inspectors were knowledgeable enough to conduct the evaluation and training. You should discuss the scenarios and quiz you intend to use with both your G-2X section and the Operational Law Attorney to ensure your own understanding of the IO issues presented and to ensure that the scenarios are applicable to your command and tailored to the mission and situations the military intelligence organizations may actually face.

For steps 7, review unit procedures, and 9, annual reviews, I used the Department of the Army G-2 checklist. Many of the sections—human intelligence, counterintelligence, signals intelligence, etc.—do not apply to these units, because they lack the equipment. However, the checklist forms an excellent basis to evaluate. During the in-brief with the inspectors, the unit should have discussed any authorities that the unit has for supporting law-enforcement and inspectors should have reviewed these written authorities. Having discussed and reviewed these authorities in conjunction with the unit’s equipment and capabilities will allow you to determine which portions of the checklist apply.

For step 8, physical checks, I checked not only their hard-copy files but also their computers and equipment. I had each military intelligence professional log on to his or her computer, both non-secure internet protocol router (NIPR) and secure internet protocol router (SIPR), and conduct a key-word search. Most of the units did not have Joint World-Wide Intelligence Communications Systems (JWICS), but appropriately cleared and read-on IGs should check the JWICS systems if available. Typical word searches included names of gangs, crime categories, force protection terms, local towns, etc. Similar to the hard-copy file review, the key-word search was an attempt to determine if the individual had collected intelligence or produced intelligence products on U.S. persons that may have violated AR 381-10. One should also check the memory of any biometric equipment or any other image-capturing equipment to determine potential violations as well.

For a sample timeline, I typically inspected one brigade per day. I conducted command interviews and the quiz / scenario discussion in the morning and then took one to two hours per S-2 section to conduct the document and file reviews. For the quiz and scenario discussion, I gathered all the S-2 sections within the brigade and conducted the discussion at one time. This approach proved more efficient; but, more importantly, it allowed the military intelligence professionals to hear the same instruction and to cross-talk among themselves about how to handle the scenarios as nested staffs.

Another question I typically receive is: “In some of our subordinate units, we only have an S-2 / 3 section, and none of them are from the Military Intelligence military occupational specialties (MOSs). Do IGs still have to inspect them every two years for IO?” The answer is yes; and, if the unit administrative section is processing the security clearances (typical for Table for Distribution and Allowances (TDA) units), the administrative section is also included in the inspection. The S-2 / 3 section of a TDA unit typically does not perform MI activities, but they may be the section to which their commander turns to discuss potential intelligence activities. Without the institutional training received by MI professionals in their professional-development courses, these S-2 / 3 personnel are more likely to fail to identify and avoid questionable activities. Therefore, the S-2 / 3 section’s IO program should at least consist of a training program on Procedures 2 (Collecting U.S. Person Information), 3 (Retaining U.S. Person Information, 4 (Disseminating U.S. Person Information), 14 (Employee Conduct), and 15 (Questionable Intelligence Activities). If the administrative section processes security clearances for the unit, then the unit IO officer should incorporate the administrative section into the IO training as well. Personnel security and the investigations conducted in support of the Defense Security Service or Office of Personnel Management are intelligence functions identified in AR 381-10, paragraph 2-2*h*. For those reasons, the S-2 / 3 section and the administrative section are subject to IG inspection to assess compliance with AR 381-10 just like any other MI unit or activity.

In sum, an IO inspection on S-2 sections is much simpler than inspecting MI units —and it is the more common inspection. S-2 sections in non-MI units typically are not only the most junior (S-2s at brigade and below are Lieutenants and their non-commissioned officers in charge are Sergeants or Staff Sergeants), but they are also isolated from other military-intelligence professionals. While they have received some IO training in their basic and non-commissioned officer education system schools, their training does not typically continue. Therefore, for them, performing the IO inspection, as outlined in this article, becomes an important part not only of their professional training but of reducing the risk of questionable activities in the command as well.