

Operations Security (OPSEC)

by Gary Williams, Senior Operations Analyst, Land Information Warfare Activity

Operations Security (OPSEC) is the only discipline that focuses primarily on unclassified information and activities. Classified information constitutes only a small fraction of the information and activities that the majority of us process every day. Most of the information we deal with is unclassified. Many wrongly think that if information or activities are not important enough to be classified, then they do not need to be protected. However, government sources estimate that 75-90 percent of our adversaries' information collection requirements can be satisfied through unclassified open sources. This article will explain what OPSEC is, what it can do for you, and how you can apply it in your unit. OPSEC is an integral element of Information Operations and Force Protection.

Too often Operations Security is just another security discipline to pile on the plate and check the block for an inspection. OPSEC is a systematic and proven process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

OPSEC complements traditional security disciplines in maintaining essential secrecy. OPSEC is threat driven, concerned with specific identified threat(s) against an activity where traditional security programs concentrate on a generalized threat and are not situation-specific. OPSEC is a fluid process that is controlled by the commander; it is not a "lock-step" program solely directed by regulations. OPSEC addresses all exploitable sources of information, not just the classified. It looks at we have to do and how we operate.

Why do we need OPSEC? All of our traditional security programs are working just fine. When is the last time someone went to jail for leaving a classified document laying out over night? When is the last time someone got a reprimand for leaving the safe open or the door unlocked? That stuff only happens to those other units. For the most part the traditional security programs are working just fine. These programs have finite requirements expressed in regulations and directives that concentrate on safeguarding classified information, and they do it quite well. What happens to the unclassified information and actions that the adversary can collect? That is the "why" of OPSEC.

Look at yourself from the adversary's point of view, not only when deployed, but at all times, from garrison through deployment, execution, and back to garrison. Following is a scenario that illustrates the potentially damaging effects of unauthorized disclosure of unclassified information. Your CONUS-based unit has been notified to deploy for a rotation to Bosnia in support of the U.S. peace operations there, and has initiated preparations. The next paragraphs discuss the possible pitfalls for OPSEC failures regarding unclassified information.

As you develop your tentative plan and conduct reconnaissance in accordance with troop-leading procedures, remember to practice OPSEC. There is no security regulation that prohibits you from throwing your unclassified trash in the garbage. Security regulations are primarily concerned with the safeguarding of classified documents. **Remember that "dumpster-diving" is the number one means of gaining espionage information and is perfectly legal according to the ruling of the Supreme Court.** No one will be court martialed for throwing out unclassified documents, nor will they receive a receipt for items taken out of their trash.

Unclassified information of a sensitive nature, improperly handled, can easily provide adversaries with valuable information on current and future operations. For example, the travel orders for "right-seat rides" with deployed unit counterparts and for site survey visits may identify the key personnel (e.g., the unit operations officer), unit, duty position, security clearance, purpose, and location of travel. The orders may be easily picked out of the trash at the landfill to find their way to a new home with a Foreign Intelligence Service (FIS).

There is no security regulation prohibiting unclassified press releases. However, there is a regulation that concerns the unauthorized disclosure of classified information. A grand jury will not indict anyone for publishing unclassified information nor will anyone get an honorable mention for their unique prose from the FIS. The FIS reads the article in the local paper that identifies your unit, mission, and deployment dates. This unclassified information verifies and adds information to the TDY orders they already have.

There are no security regulations that prohibit the discussion of unclassified information over a telephone – regulations do prohibit the transmission of classified information on unauthorized telephones. Soldiers do not go to jail for discussing unclassified information over the telephone, nor do they receive thank-you notes for their assistance in the information-

gathering endeavors of our adversaries. In our Bosnia scenario, the FIS decided to listen for more information on trans-Atlantic telephone circuits, based on information already collected from the notified unit. The FIS recorded all of the unclassified information the S-3 discussed with Task Force Eagle to coordinate the trip. This is the third piece of unclassified information the adversary collected – he now knows more details of the unit's mission than the troops do!

There are no security regulations that prohibit displaying distinctive clothing or emblems. Soldiers do not get Article 15s for displaying unit distinctive items while traveling, nor do they receive a letter of appreciation from the FIS for making accurate identification so easy for our adversaries. In our Bosnia scenario, the FIS easily identified the S-3 at the airport by the distinctive unit logo sticker on his laptop case.

There are no security regulations that prohibit leaving unclassified documents in a car. However, there is a regulation for the proper safeguarding of classified documents. In our Bosnia scenario, the S-3 will not go to federal prison for leaving unclassified documents in his rental car while TDY enroute to or from the theater of operations. However, the same intelligence service that identified him at the airport subsequently burglarized his rental car when he stopped for dinner. This is the final confirmation of unit plans they needed.

Why Operations Security? In the Bosnia scenario presented above, not one piece of classified information was disclosed, and yet adversaries were able to piece together enough unclassified sensitive information to paint a clear picture of the unit's mission and operations. Our scenario demonstrates why effective OPSEC is so important. All of the information that was unintentionally disclosed to the hypothetical adversary was either unclassified documents or activities. Could all of this happen to one unit and one mission? Perhaps. Do not discount the events in the scenario presented above – every one of these situations has actually happened at one time or another.

How could an effective OPSEC program have saved this mission from compromise? Applying the OPSEC process to the hypothetical Bosnia scenario will provide some answers.

The OPSEC process consists of five steps.

Step One – Identify Critical Information. Identify what information has to be protected and for how long. What critical information does the adversary require with enough time to collect and analyze it to be detrimental to your operation? The questions you are asking are Essential Elements of Friendly Information (EEFI). Answers to EEFI are critical information. Some examples for our Bosnia scenario might be:

- What units will rotate to support TFE?
- What is their specific mission?
- When will the unit deploy and where will the unit be located?

Compare these answers to your Security Classification Guide if the information is classified. Then you have perfectly good traditional security programs to protect it. You need OPSEC to protect the unclassified information and observable activities that indicate or disclose the critical information.

Step Two – Threat Analysis. Identify your threat. Determine their collection capabilities. Request this information through your intelligence channels. Most of the collection techniques in the scenario concerned HUMINT. The phone intercept was Signals Intelligence (SIGINT) and the press release is Open Source (OSINT). Let us assume that all of the unclassified information above was collected.

Step Three – Vulnerability Analysis. Look at your planned operation. Identify what observable actions, indicators, or information is vulnerable to collection by your adversary. Determine what protective measures you can use to reduce this vulnerability. The most desirable protective measure provides the needed protection at the least cost to operational efficiency. There are three types of measures that you can apply. **Action Controls** eliminate the indicator. **Countermeasures** attack the adversary collection system by using camouflage, concealment, jamming, and physical destruction. **Counter Analysis** provides a possible alternative for the intelligence analyst. Try to confuse the adversary analyst through deception and cover. Select at least one measure for every vulnerability.

Step Four – Assessment of Risks. The purpose here is to identify the best OPSEC measures to use. Only the commander can make this decision. He must balance the operational failure against the cost of the measure. He must consider: What is the impact of the measure to operational efficiency? What is the risk to mission success if he does not implement the measure? What is the risk to mission success if the measure does not work?

Step Five – Application of appropriate measures. This is where the measures chosen by the commander will be applied to ongoing activities and incorporated into future plans. Operations plans, orders, or an OPSEC plan direct the measures that soldiers, civilians, and government contractors have to implement.

Having assessed the threat and identified the risks involved in our Bosnia scenario, here are some OPSEC measures that could have prevented unauthorized disclosure of sensitive, unclassified information.

- The travel orders could have stated "training coordination" or some other innocuous reason and not made any mention of the "site survey for unit rotation to Bosnia." Be careful how much information is provided on travel orders or any other documents. Establish a policy that "office waste" is destroyed and not put into the trash or recycled.
- If a press release is necessary, review it to ensure it does not disclose any critical information. Press releases, SOPs, and Freedom of Information Act responses should automatically be reviewed by the OPSEC Officer.
- Do not discuss or transmit any critical information over an unclassified means; use a secure telephone, fax, or e-mail. Do not discuss critical information with anyone who does not have a "need to know." Post a list of EEFI near every telephone, fax, and computer terminal, and mess hall, office, latrine, etc., to remind everyone what not to discuss or transmit.
- Do not wear distinctive items of clothing or display emblems that identify your unit if this information is critical.
- Safeguard sensitive information the same way you would safeguard classified. Do not leave it in your vehicle, your hotel room, or office. Properly mark all critical unclassified information and establish safeguard procedures.
- Practice a little camouflage and concealment, not to mention common sense. Institute an OPSEC training and awareness program within your unit.

The OPSEC process has to be applied all of the time to all activities; it needs to be applied from the initial planning stages. In the Bosnia scenario presented above, the mission and operation were vulnerable to compromise at any point by any person. The Commanding General could make an "off-the-cuff" remark during a press conference; a soldier purchasing extra cold-weather gear at a military surplus store could innocently mention that his unit was going on this mission. Practicing effective OPSEC is a continuous effort that requires self-discipline and command emphasis to train soldiers and leaders to "think OPSEC."

There are some basic requirements in **Army Regulation 530-1, Operations Security (OPSEC)**:¹ OPSEC is an operations function, an OPSEC Officer will be appointed in writing down to and including the battalion level, and unit OPSEC programs will address the six common areas at a minimum:

- Appointment of an OPSEC officer.
- Provide OPSEC planning guidance.
- Apply systematic OPSEC analytical techniques.
- Establish OPSEC awareness and training guidance.
- Conduct annual OPSEC review.
- Establish procedures for cross command and agency coordination.

Start the process to improve your unit OPSEC program by consulting your OPSEC Officer in the Battalion S-3 shop. Apply the process beginning right now. You cannot learn how to do it unless you use it! Stick to the basics. You can also obtain more information from the Operations Security Professionals Society at <http://www.opsec.org>.

Note:

1. Headquarters, Department of the Army, **Army Regulation 530-1, Operations Security (OPSEC)** (Washington DC: USGPO, Unclassified, Distribution Limited), 3 March 1995.
