

## OPS Professional Standards Committee

### Documenting the OCP Applicants' Understanding of the OPSEC Process

The Professional Standards Committee review of papers submitted for OCP has found that at least a few do not meet established criteria for determining an applicant's understanding of the OPSEC process. Below are extracts from a variety of sources and our associated comments that should be expressed in some form in an OCP paper to fully represent an OPSEC point of reference and thus reflect the OPSEC process. Note that we do not suggest that what is presented below be copied verbatim but that the ideas, processes, and meanings should be readily identifiable in an applicants OCP paper.

OCP Papers should conform to the context of the term OPSEC. For example, the OPSEC practitioner believes that *“Operations security (OPSEC) is concerned with identifying, controlling, and protecting the generally unclassified evidence that is associated with sensitive operations and activities.”* We interpret this to mean, identifying what an adversary can see, hear, or otherwise discern **about us** for their purposes and to our detriment. Terrorists, of course, are seeking targeting information to ensure their successful attack, criminals to enable their fraud or their theft of items of value, insurgents and adversary military forces to thwart our operations/activities or to take some action to do us harm, and so forth.

In a military context which one can also translate into an appropriate civilian environment, “Operations Security (OPSEC) is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- a. identify those actions that can be observed by adversary intelligence systems;
- b. determine what indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and,
- c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.”

**“OPSEC’s most important characteristic is that it is a process and not a collection of specific rules and instructions that can be applied to every operation or activity.**

Therefore, OPSEC programs and security programs must be closely coordinated to ensure that all aspects of sensitive operations are protected.”

The Professional Standards Committee interprets this to mean that OPSEC concerns itself with what we are doing that gives a discerning adversary the insights to our activities sufficient to do us harm. For example, do we do the same things the same way every time (SOPs)? Stereotypical activities may constitute an exploitable weakness. We use an adversary perspective to make assessments of our activities. OPSEC practitioners promote the idea of looking at ourselves as an adversary would look at us.

Many OCP applicants consider the concepts stated above in their OCP papers but do not clearly present their material in an OPSEC framework. Using the OPSEC model and fitting a presentation or an OCP paper to that model more readily enables others to understand a writer's contribution to a better understanding of OPSEC and/or the actions necessary to improve an organization's OPSEC posture.

In considering an OCP paper, we match what is written in a paper to the accepted OPSEC model (which of course is a risk management model). The OPSEC model consists of five distinct steps (actions): identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate OPSEC measures. We recognize that these steps are iterative in nature with feedback loops that continually add new data as received such as changes in the threat, vulnerabilities or consequences. The OPSEC process should not be a static process. Nonetheless, the recognized five steps are usually presented in the order above to promote a better understanding of the process. It is logical to assume that one would determine: (1) what is important to protect and why—ID the critical information; (2) from whom—ID the threat/adversary; (3) exploiting what—ID the vulnerabilities; (4) using these three elements to determine risk levels—thus making a risk assessment; and finally, (5) determining how to reduce that risk to an acceptable level— application of appropriate OPSEC measures.

**Critical information** is defined as: Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (Joint Pub 1-02). **Operations security indicators** are friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (Joint Pub 1-02) An **operations security vulnerability** is a condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (Joint Pub 1-02) **Operations security measures** are the methods and means to gain and maintain essential secrecy about critical information. The following categories apply to OPSEC security measures:

- a. action control. The objective is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake; decide whether or not to execute actions; and determine the “who,” “when,” “where,” and “how” for actions necessary to accomplish tasks.
- b. countermeasures. The objective is to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering and processing capabilities.
- c. counteranalysis. The objective is to prevent accurate interpretations of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers. (Joint Pub 1-02)

Here is what the Interagency OPSEC Support Staff (IOSS) states:

### **”What can I do to Help Thwart any Further Attempts to Harm the U.S.A.?”**

We can all incorporate OPSEC into our everyday work routine. Practicing operations security will help you accomplish your goals. When you do something, ask yourself, "What could an adversary glean from the knowledge of this activity? Is it revealing information about what we do and how we do it?" It is helpful to view yourself and what you're doing as an adversary would. For example, what can be gained by observing your actions or reading what you place on a website?

Use examples to illustrate the points made to support your understanding of the OPSEC process. You may use business or military or federal agency examples. Research your examples. For example, you might build on a real world example as: *Exfiltrations of unclassified data from [the defense industrial base's] unclassified systems have occurred and continue to occur, potentially undermining and even neutralizing the technological advantage and combat effectiveness of the future force, reads an Aug. 15, 2008 information paper on the Army's concerns about the security of controlled unclassified information.* (cite the specific source of this selection) Or an industry example e.g., Colonel Harland Sanders' handwritten recipe of 11 herbs and spices is considered one of the country's most famous corporate secrets. So important to the company is the 68-year-old concoction that coats the chain's Original Recipe chicken that only two company executives at any time have access to it. The company refuses to release their name or title, and it uses multiple suppliers who produce and blend the ingredients but know only a part of the entire contents. (cite the specific source of this selection)

Finally, the OCP paper represents the applicants' professional knowledge and experience. As such, the paper should be grammatically correct, professionally organized, and focused.

**The OPS Professional Standard's Committee hopes that this short** discussion of OPSEC will assist those preparing OCP papers in better addressing OPSEC and thus to demonstrate knowledge of the OPSEC process as required by the OPS OCP certification process.