What is opsec and why do we have it

Law, Security

What is OPSEC and Why Do We Have It What is OPSEC? It’s a process of protecting little pieces of information that might grouped together to give the bigger picture. It is also protecting critical information deemed mission essential for military commanders. It is simply denying your adversary the information that they might need to harm you or the mission. The AR that covers OPSEC is AR 530-1 and goes over purposes, responsibilities, policy, procedures, training requirements, OPSEC review, assessment, survey, contract and subcontract requirements and special access programs.

The reasons why we have OPSEC is because any vital information that the enemy can get their hands on can give them an advantage on the battle field or operations. Those little pieces of information could show the enemy the full picture of what it is that we plan to execute. Most don’t know what is considered vital information. Think about it, what would you like to know about your enemy and how to infiltrate, interfere or stop their objective. How about where you are going, when you are going, how are you moving, what equipment that you will be using and even what paths have you taken before.

Even your unit’s job association can be a part of the information they can gather on. Certain identifying marks such as your unit patch, or any other unit/ battalion identifiers can even give information. For instance the enemy is looking at the patch and can look up throughGoogleand find out what unit you are with and keep open eyes and ears to see if they can get any information on what your purpose is and where you will be. Even taking pictures in certain places can give the enemy a layout of an area.

It’s not wise to take pictures of equipment, it would not be hard with the information highway to find out all they need to know about certain functions of our equipment and their weak spots as well. In this day in age we have thesocial medianetwork that can also help the enemy track and get information. How OPSEC affectsfamilyandsocial networkingWe all have friends and family that want to know what you are doing but there are only so many things that you can tell them without violating OPSEC.

You are not the only one who needs to understand why there is OPSEC, your family needs to understand its importance as well. Any information you give them and they put out there can affect you and them. The military offers family members who are curious about OPSEC classes and briefs at the FRG meetings. They go over what it stands for and why it’s so important in the military. There are also links on the internet that explain and answers a lot of questions they may have.

There is also a Facebook page that family members can go on, it’s called Army Operation Security. Your family has to understand that there is only so much you can tell them and even what you do tell them they don’t need to be telling others or posting it on Facebook. Without thinking they could accidently put the information out without knowing if the person they told is the enemy or a spy. You know what they say keep your friends close and keep your enemies closer.

The enemy thinks the same way and will do whatever it takes to get the information they need to plan and infiltrate our operations. Families are the biggest target for our enemies to infiltrate and get information. One more

important thing to think about is the enemy could be anyone, American or even your family you never know. There are many reasons why we have OPSEC but not taking the proper measures can result in serious injury or death to personnel, damage to weapons systems, equipment and facilities, loss of sensitive technologies and missionfailure.

The process of OPSEC There is a process to OPSEC as well the subjects that are covered are identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, an application of appropriate OPSEC measures and assessment of insider knowledge. Identification of critical information is the process of identifying what information is needed by the enemy, not so much protecting everything that is classified or sensitive unclassified, but protecting what is more vital and would be more useful to the enemy.

Analysis of threats is the research and analysis of intelligence, counterintelligence and open source information on the likely enemies of a planned operation. Analysis of vulnerabilities is to examine each and every aspect of the planned operation and try to identify certain OPSEC indicators that could reveal critical information and then compare those indicators with the enemy intelligence collection capabilities used in the previous actions that they have taken in the past.

Assessment of risk is where they first analyze the vulnerabilities identified in the previous action and see what OPSEC measures can be taken to prevent the opportunity of the enemy getting information, and then those measures are selected for execution based upon a risk assessment done by the

commander and staff. Application of appropriate OPSEC measures is when the command implements the OPSEC measures selected in the assessment of risk, action, or in the case of planned future operations and activities, which includes the measures in specific OPSEC plans.

Assessment of Insider Knowledge is assessing and ensuring employees, contractors, and key personnel having access to critical or sensitive information practice and maintain proper OPSEC measures by organizational security elements; whether by Open Assessment or Covert Assessment in order to evaluate the information being processed and / or handled on all levels of operation ability (the employees/mid-level/senior management) and prevent unintended/intentional disclosure. These are all important steps that are taken to implement those measures to use as soldiers.

All this information that they gather and analyze gives us the understanding of what the enemy is looking, what they have done in the past and what they may plan in the future. We have briefs annually that go over such information that they gather and the measure to prevent them from happening again. We even sign a nondisclosure agreement after we are briefed on what we are not supposed to do when we have information that is mission critical. Basically they go over the does and don’ts in this brief and we are bound in contract not to disclose any of this information to whom it doesn’t concern.

Later in this essay, you will know the consequences to violating the nondisclosure agreement. Indicators and Vulnerabilities There are other forms of analyzing ways that the enemy would get information and create

weak spots in our operations or mission tasks, they are Indicators and Vulnerabilities. Indicators, consists of five characteristics which are signatures, associations, profiles, contrasts and exposures. A signature can cause certain indicators to be identifiable and stand out.

If a signature is unique and stable, it reduces the unclear and uncertainty of a particular indicator and reduces the number of additional indicators that must be observed in order to determine the significance. If the indicator's signature is stable, meaning that the behavior is constant and repeated, an adversary may accurately predict future actions. By varying the pattern of behavior, the signature's stability can be interrupted and increase the uncertain information of an enemies observations. An association is the relationship that an indicator has to other information or activities.

Adversarial Intelligence Analysts spend a considerable amount of time comparing current observations with past observations, which may reveal possible relationships. For example, an observer may note a particular employee report to work after hours. Though previousobservation, the Analyst is aware of that employee's position as an on-call computer forensics analyst. Given the association between those two observations, the Adversarial Intelligence Analyst could conclude that the organization has suffered a computer breach of some sort.

An association can also take the form of a pattern. For instance, if it is observed that we do a test fire on our weapons before rolling out the gate to go on mission, an analyst may be able to accurately predict these procedures. Lastly, an association can take the form of organizational

patterns, particularly in military units. The analyst may be aware that a particular unit is comprised of Headquarters Company, a maintenance company and a transportation company.

If one of these elements is detected, the presence of the others would be strongly suspected. A profile is the sum of multiple signatures, and what that means is when multiple signatures are detected, the combination therein would be more or less unique to a particular mission or task. For instance, if signatures are detected that indicate that aircraft fueling capacities are in place, as well as air traffic control, personnel and weaponry, a profile can be compiled indicating future air-based operations.

If a unique profile is observed, an analyst may be able to accurately determine which type of operation is in progress, minimizing the need for additional observation and analysis. Contrasts are any differences between the established pattern and current observations. Contrasts are the most reliable indicators because they depend on differences in established and repeated profiles, and need only to be observed rather than understood. A contrast can take many forms; for instance leaving work at a different time or the presence of vehicles or aircraft that were not previously observed.

When noting a difference, the analyst will attempt to determine if the change is isolated or widespread, if the change has occurred previously (and has a matching association), if anything significant has occurred since the change and what the change may represent. The exposure of an indicator refers to the length of time and the time frame in which the indicator is observed. If an indicator is allowed to be observed for a long period of time, it will be

assimilated into the profile and be assigned a meaning. If an indicator is able to be observed for only a short period of time and does not repeat, it is less likely to attract attention.

However, if the indicator is observed for short periods of time, but is repeated frequently, it will begin to be seen as a contrast to a normal profile. These can be found on OPSEC professionals. com. Vulnerabilities, is the information and indicators that can weak spots to infiltrate and disrupt the mission plans or operation. Finding and preventing the vulnerabilities can reduce the affect that it may have on missions and operations that are planned and executed. For instance, your path that you take to a given destinations, and the terrain were they could plant IED’s.

If someone was to give out information as to where the mission was going and when, it could give the enemy the time to organize a plan of attack on that convoy or mission of operation. Convoy and Equipment security Convoy security is a very important part of our job and there are techniques that we have in the way we pull security and make ourselves less known to the enemy as well. For example, when we have to halt the convoy for complications that arise, we will turn off our lights to make ourselves less know. We also, put spaces between us to eliminate more damage in the event that we are hit with either small arms fire or an IED.

Identifying marks on the vehicle is not permitted because it can be traced and monitored by the enemy and observe and predict the way we move and how we operate. These techniques that we have shouldn’t be spoken to anyone as well. If the enemy was to know this information it would give us

an even more disadvantage in completing our mission. Even the classes that we take like (Crow, Puma, Crew, etc.) should not be shared information, the enemy would love nothing more that to understand our equipment and the way it works.

They will try to find the weakness in anything that we use to plan, secure, and complete our missions and tasks. Radio frequencies are another very important part of information that could be very valuable to the enemy. With that information they could pretty much get just about anything that they would possible need to know to infiltrate us, harm us, equipment and the very mission itself. All this information and more is vital to our very purpose here and simply if the person to whom at anytime you are speaking with or if there are others around and they do not need to know don’t say anything.

One other thing that is important to remember there are a lot of DOD contractors around that know and understand about OPSEC, and they are listening around you and will report this information that they hear. Even our battle drills we go over on how we respond and operate under certain conditions can be considered valuable information to the enemy, and something they could use against us. How to Conduct an Operations Security (OPSEC) Assessment OPSEC Assessments are conducted to evaluate an adversary's or competitor's ability to access your critical information, intellectual property, proprietary information or personal information.

OPSEC Assessments directly benefit anyone desiring to protect information or assets from disclosure. Operations Security (OPSEC) Assessments enable insight to your predictable indicators, exploitable processes and procedures

while presenting specific measures to counter potential vulnerabilities. Assessments can be conducted by internal representatives from each department or can be performed by external experts and typically run from 1-3 weeks.

Step 1: Identify information critically important to the organization, mission, project or home [intellectual property, mission details, plans, R&D, capabilities, degradations, key personnel deployment data, medical records, contracts, network schematics, etc.] Step 2: Identify the relevant adversaries, competitors or criminals with both intent and capability to acquire your critical information. Step 3: From the adversary's, competitors, or thief's perspective, identify potential vulnerabilities and means to gains access to results of step 1. Interviewa representative sample of individual.

Step 4: Assess the risk of each vulnerability by its respective impact to mission accomplishment / performance if obtained Step 5: Generate / recommend specific measures that counter identified vulnerabilities. Prioritize and enact relevant protection measures. Step 6: Evaluate measure effectiveness, adjust accordingly. This was reference at http://www. wikihow. com/Conduct-an-Operations-Security-%28Opsec%29-Assessment There are many tips when conducting a Operations Security (OPSEC) Assessment here are a couple. Don’t try to perform all analysis on your own, obtain threat data from the experts.

The cost of OPSECmoneywise would be prohibitive to attempt to protect information that is already accessible to the public so focus on what you can protect than what is already publicly accessible. Even though 100%

awareness of OPSEC is realistic, zero vulnerabilities are not. Your critical information list should not be secret and inconspicuously posted near PC monitors, phones, copiers, etc. You should keep your list to about ten items. Those aware of what to protect have a better chance of protecting sensitive information as opposed to those unaware of its value is a general rule.

Regular assessments ensure your best protection. OPSEC often provides low cost solutions to high tech problems. Instead of a long drawn-out report on observations, findings and proposed counter measures can be formatted in a presentation template. To mitigate vulnerabilities you should include a plan of actions and milestones (POA&M) in the brief to decision makers. Consequences to violating OPSEC There are many consequences to violating the nondisclosure statement that all soldiers, NCO’s and Officers are obligated to adhere and follow. This is a direct order from your chain of command.

This statement informs you of the obligations and responsibilities concerning OPSEC procedures and consequences that will occur if violating this statement. OPSEC involves vital and important information on mission operations. This includes dates, times, cargo, number of personnel and vehicles, even the rout and destinations of missions. Violations of OPSEC can happen many different ways especially with currenttechnology. Cellular phones are the easiest and most convenient method of use getting and giving information. However, another method would be the internet.

People who make random posts on facebook or other forms of social media pages or write blogs about things they do in combat areas reveal types of

information without realizing what they have done. Revealing this type of information, whether it was intentional or not can have severe consequences from the Military Judicial System. These consequences include UCMJ, Article 15, Military Court Martial, and separation from the military and loss of all VA benefits. Another and more substantial result of the violations is the loss of people’s lives because the enemy found this information from unsecuredcommunicationnetworks.

The first course of punishment is an Article 15 of the UCMJ. A Soldier will receive the maximum punishment from an Article 15. Which would be 45 days extra duty, 45 days of restriction, loss of pay and reduction of rank. If the information the Soldier revealed results in the convoy getting ambushed and Soldiers die, that Soldier may have to appear before a Military Court for a Court Martial Hearing. If the Courts finds the Soldier guilty of the charges they have been accused of. This will result in a Dishonorable Separation from the Military.

A Dishonorable Separation from the Military may result in future difficulties in civilian life after you are released from the Military. The main problem might be trying to attain a civilian job. When employers see a dishonorable discharge from the military service and the reasons to which you obtained this action. They will be less likely to employ such a person who they can’t trust in. Along with the dishonorable discharge, you will loss all benefits and entitlements. The Bureau of Veteran affairs will also give soldiers loans to buy a house or brand new vehicle.

This will also be taken from, because due to the soldier’s indiscretion to reveal vital information and risk the lives of their fellow comrades. References Operation Security on Wikipedia: http://en. wikipedia. org/wiki/Operations_security Operation Security AR 530-1: www. fas. org/irp/doddir/army/ar530-1. pdf OPSEC Indicators: www. opsecprofessionals. org/articles/indicators. htm How to Conduct an Operations Security (Opsec) Assessment: http://www. wikihow. com/Conduct-an-Operations-Security-%28Opsec%29-Assessment