

OPERATION SECURITY (OPSEC)



“In the wild, the wolf studies his prey; prowling and studying until he finds a vulnerability- then he attacks.”

What is OPSEC?

Operation Security is a process to deny adversaries information about friendly intentions and capabilities, which they need to make effective and timely decisions. It does not only deny our adversaries classified information but critical information as well, which is always sensitive and often unclassified.



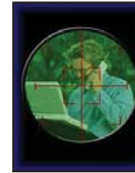
“Like a wolf, America’s enemies are looking for vulnerabilities and waiting to attack us.”

Who’s the adversary?

Our adversaries are no longer the traditional threat from the Cold War era. Granted there is still the Foreign Intelligence Services (FIS) threat from the different countries around the world, but our adversaries come

from all sources. Some examples include but not limited to are:

- Competitors
- Hackers
- Criminals
- Insiders
- Terrorists



Basically anybody who has the intent and ability to collect and use our information against us is an adversary.



What are they after?

According to an Al Qaeda Training Manual, their operatives are to acquire any information regarding:

- Leave Policies.
- Brigades and names of companies.
- Unit strengths.
- Names/photographs of important people.
- Present and future US capabilities.
- Amount of lighting used.
- Weapons used.

FACT: Over 80% of all terrorist planning information was provided by the target.

FIS are increasingly likely to target members of the technical community including engineers, regardless if they have a security clearance or not. The US spends millions of dollars in research and development on new technology. Why would another country spend that much for the same product when they could just obtain the information at a fraction of the cost or for free from the people working with it?

That FIS’s country takes that information and reproduces a cheaper product than the US, because they do not have to try to recover the research and development costs. This results in loss of revenue and ultimately jobs, even yours. Then again, it does not just have to be a foreign country; it could be a business rival.

FACT: More than 75% of our adversaries’ intelligence needs come from unclassified sources.

In today’s world of global acquisition where so much information is available at a stroke of a key, unclassified information has taken on an entirely new importance. The internet is not the only source our adversaries use to collect on us. Other open sources available are:



- Newsletters
- Television
- Surveillance
- Social Engineering
- Trash



The role OPSEC must play in our organization has never been more important than it is today and will be in the future. It is what helps us to protect and maintain the technological advantage we have.

Remember: All military operations depend upon some form of technological advantage we currently have for mission success!

This is especially true since more and more of the US military systems have become more technological. The loss of militarily critical technology can result in surprise on the battlefield and a loss of US lives from our own technology. The acquisition of sensitive technology by our adversaries has led to the significant enhancement of their military-industrial capabilities at the expense of the US and our most precious resource, our warfighter!



“With every glimpse we give them, they gain an advantage. To ensure America’s victory over her adversaries, we must think like them – like the wolf.”

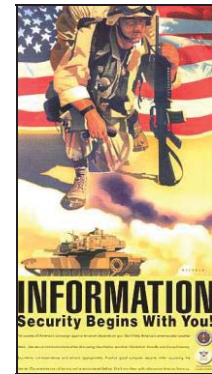
What can I do?

There are many things that you could do to apply OPSEC in your everyday procedures. Things like:

- Shredding Sensitive but Unclassified paperwork, such as alert rosters, work orders or technical manuals.
- Reporting suspicious activities on or near the installation to the Security Division.
- Not wearing your security badge outside the installation.
- Practice “Need-to-Know”. Only share information with those that have a need to know the information in accomplishing our mission.
- Start “Thinking Like the Wolf”



Mind you that we cannot and should not attempt to keep everything secret, but those bits of information that are “nice to know” for our adversaries need to be limited as much as possible. Remember, the adversary doesn't need just classified information; the disclosure of certain types of unclassified information can be just as damaging to our operation. OPSEC incorporates everyone, from the commander to the individual on an assembly line. The warfighter depends on us to give them the technological edge!



For Additional OPSEC information contact your OPSEC Officer at x58660.

References:

AR 530-1, DA Operation Security
 1st Information Operations Command
https://opsec.1stiocmd.army.mil/io_portal/Public/Pages/Sections.cfm?section=opsec