OPSEC Glossary

Term/Acronym	Definition
Adversary	An individual, group, organization, or government that must be denied critical information. An adversary is synonymous with an enemy.
Countermeasures	Employing devices and/or techniques that has as its objective the impairment of the operational effectiveness of an adversary's activities. Countermeasures may include anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities.
Critical Information	Specific facts about friendly intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly missions.
Explosive Ordnance Disposal (EOD)	A team of highly trained, specifically skilled personnel who execute processes by which hazardous explosive devices are rendered safe.
Indicator	Anything that draws attention to critical information or gives an adversary a clue about what's going on.
Operations Security (OPSEC)	An analytic process used to deny an adversary information, generally unclassified, concerning intentions and capabilities by identifying planning processes or operations. Operations Security does not replace other security disciplines; it supplements them. The OPSEC process includes the following five steps: (1) identify critical information, (2) identify the threat, (3) assess vulnerabilities, (4) analyze the risk, (5) develop and apply countermeasures.
Operations Security Countermeasures	Methods and means to gain and maintain essential secrecy about critical information.
Operations Security (OPSEC) Process	Analytical process that involves five components: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.
Risk	A measure of the potential degree to which protected information is subject to loss through adversary exploitation.
Risk Analysis	A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios to determine the likelihood of compromise to critical information.
Risk Assessment	A process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss.
Sensitive Information	Information that the loss, misuse, unauthorized access, or modification of could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code, but that has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of National defense or foreign policy.
Threat	The existence of an adversary with intent and capability to gain unauthorized access to critical information and to use that information to the advantage of the adversary or to harm us.
Vulnerability	A weakness an adversary can exploit to get critical information. Anything that might make critical information available to an adversary.