OPSEC Fundamental for OPSEC Practitioners

Glossary & Acronyms

CDSE training

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

Back to Top

B

Back to Top

C

Common Access Card (CAC)	
Commander in Chief, Pacific Command (CINCPAC)	
Counterintelligence	Efforts to identify, assess, and counter threats posed by foreign intelligence entities and insider espionage.
Countermeasures	Actions taken to prevent adversaries from detecting, interpreting, or exploiting critical information.
Controlled Unclassified Information (CUI)	Information that requires safeguarding or dissemination controls pursuant to law, regulation, or government-wide policy.
Critical Information & Indicators (CII)	Observable clues or pieces of data that could lead an adversary to infer critical information.
Critical Information and Indicators List (CIIL)	
Critical Infrastructure Protection (CIP)	Critical Infrastructure Protection (CIP)
Cybersecurity	Protection of DoD information systems and networks from digital threats and cyberattacks.

Back to Top

D

Department of Defense (DoD)	

Back to Top

E

Back to Top

F

Back to Top

G	

Back to Top

H	
Human Intelligence (HUMINT)	

Back to Top

I	
Industrial Security	Protection of classified information in the hands of cleared defense contractors.
Insider Threat	Risks posed by trusted individuals who may intentionally or unintentionally harm national security through unauthorized disclosure, sabotage, or other malicious acts.
Interagency OPSEC Support Staff (IOSS)	A former national-level OPSEC training entity under the NSA, disbanded and replaced by the National Operations Security Program (NOP).

Back to Top

J	
JCS Publication 18	The first formal doctrine for Operations Security, published by the Joint Chiefs of Staff in 1973.
Joint Chiefs of Staff (JCS)	

Back to Top

K	

Back to Top

L	

Back to Top

M	
Military Deception	Operational activities designed to intentionally mislead adversaries about DOD capabilities, intentions, or operations.

Back to Top

N	
National Operations Security Program (NOP)	A national-level office under the ODNI responsible for OPSEC oversight and training.
National Security Agency (NSA)	

N	
National Security Decision Directive (NSDD) 298	The first national-level OPSEC policy signed in 1988, establishing OPSEC training and oversight.
National Security Presidential Memorandum (NSPM) 28	The updated national-level OPSEC policy signed in 2021, expanding OPSEC requirements to all federal departments and agencies.
Non-Traditional Collector	An individual not formally trained as a spy but expected to work in the best interest of their homeland, often in academic or professional settings.

Back to Top

O	
Office of the Director of National Intelligence (ODNI)	
Operations Security (OPSEC)	A security discipline designed to deny adversaries the ability to collect, analyze, and exploit information that might provide an advantage against the United States.
OPSEC Cycle:	A continuous process involving five steps: identifying critical information, analyzing threats, analyzing vulnerabilities, assessing risks, and applying countermeasures.
OPSEC Working Group	A collaborative team of subject matter experts from various disciplines to identify critical information, assess vulnerabilities, and determine countermeasures.
Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)	

Back to Top

P	
Physical Security (PhysSec)	Measures to safeguard personnel, facilities, and resources from unauthorized access, damage, or loss.
Purple Dragon	A classified study conducted during the Vietnam War to investigate how adversaries were gaining intelligence on U.S. operations, leading to the formal establishment of OPSEC.

Back to Top

Q	

Back to Top

R	
Risk Assessment	Evaluation of the likelihood and impact of adversaries collecting critical information, used to justify countermeasures.

Back to Top

S	
Signals Intelligence (SIGINT)	
Special Access Program (SAP)	Enhanced security measures for highly sensitive programs requiring extraordinary protection.

Back to Top

T	
Tactics, Techniques, and Procedures (TTPs)	
Threat Analysis	The process of identifying potential adversaries and their capabilities and intentions to collect, analyze, and exploit critical information.

Back to Top

U	

Back to Top

V	
Vulnerability Analysis	The process of identifying weaknesses that adversaries could exploit to gain critical information.

Back to Top

W	

Back to Top

X	

Back to Top

Y	

Back to Top

Z

Back to Top