THE TEXAS A&M UNIVERSITY SYSTEM

UCAH OSPEC Awareness

Zach Carwile; Deputy Chief Research Security Officer, The Texas A&M University System | 17 May 2021

Operational Security (OPSEC)

- Operations security (OPSEC) is a process by which organizations assess and protect public data about themselves that could, if properly analyzed and grouped with other data by a clever adversary, reveal a bigger picture that ought to stay hidden. It's a discipline of military origins that in the computer age has become vital for government and private organizations alike.

- Source: What is OPSEC? A process for protecting critical information | CSO Online

OPSEC Process

- The OPSEC process is a systematic method used to identify, control, and protect critical information (Source DoD 5205.02)
- Participation in the UCAH will require familiarity and adherence to an OPSEC plan developed in concert with DoD.
- Upon completion, this plan will be made available to UCAH members and participants for review.

OPSEC Process

- Identify Critical Information
- Conduct a Threat Analysis
- Conduct Vulnerability Analysis
- Conduct Risk Assessment
- Apply OPSEC Countermeasures

Source: DoD Manual 5205.02

Critical Information (CI)

- Critical information is information about DoD activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources.

Source: DoD Manual 5205.02

Conduct a Threat Analysis

- Threat information is necessary to develop appropriate countermeasures. The threat analysis includes identifying potential adversaries and their associated capabilities and intentions to collect, analyze, and exploit critical information and indicators. A thorough threat analysis will answer the following questions:
  - ❑ Who is the adversary? What is the adversary's intent and capability?
  - ❑ What are the adversary's goals?
  - ❑ What tactics does the adversary use?
  - ❑ What does the adversary already know about the unit's mission?
  - ❑ What critical information has already been exposed and is known by the adversary?

Source: DoD Manual 5205.02

Conduct a Vulnerability Analysis

- An OPSEC vulnerability exists when the adversary is capable of collecting critical information or indicators, analyzing it, and then acting quickly enough to impact friendly objectives. Conducting exercises, red teaming, and analyzing operations can help identify vulnerabilities.

- Source: DoD Manual 5205.02

Conduct a Risk Assessment

- The risk assessment is the process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss. It involves assessing the adversary's ability to exploit vulnerabilities that would lead to the exposure of critical information and the potential impact it would have on the mission. Factors to consider include:
  - ❑The benefit and the effect of the countermeasure on reducing risk to the mission.
  - ❑The cost of the proposed countermeasure compared with the cost associated with the impact if the adversary exploited the vulnerability.
  - ❑The possibility that the countermeasure could create an OPSEC indicator.

Source: DoD Manual 5205.02

Apply OPSEC Countermeasures

- Countermeasures are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary's collection system. If the amount of risk is determined to be unacceptable, countermeasures are then implemented to mitigate risk or to establish an acceptable level. Countermeasures should be coordinated and integrated with other IO core capabilities if applicable.

Source: DoD Manual 5205.02

THE
TEXAS A&M
UNIVERSITY
SYSTEM