WHAT IS OPSEC?

Operations Security (OPSEC) is an analytical process used to deny an adversary information about our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning process or operations.

As government employees, military members, and contractors the American people trust us to do our jobs and keep them safe. The mishandling of information can put everything at risk.

Often, the information that is used against us is not classified; it is available to anyone who knows where to look and what to ask. Predictable routines, casual conversations, routine acquisitions, and online behavior could provide our adversaries with the information they need to do us harm.

LEARN MORE

The Interagency OPSEC Support Staff (IOSS) provides OPSEC consultancy services, training, awareness products, and assessments to U.S. government departments and agencies and contractors with OPSEC requirements.

The IOSS assists customers in developing and managing their OPSEC programs to achieve and maintain self-sufficiency through technical guidance and assistance customized to the customers' needs.

The IOSS offers web-based training, instructor led online training, classroom training, DVDs, posters, and other awareness products on topics such as OPSEC fundamentals, public release decisions, analysis, program management, contracts, social media, and cyber. Products are available at no-cost.

MP2193326AB

Visit www.IOSS.gov
Contact us at ioss@radium.ncsc.mil
Or call us at 443.479.4677

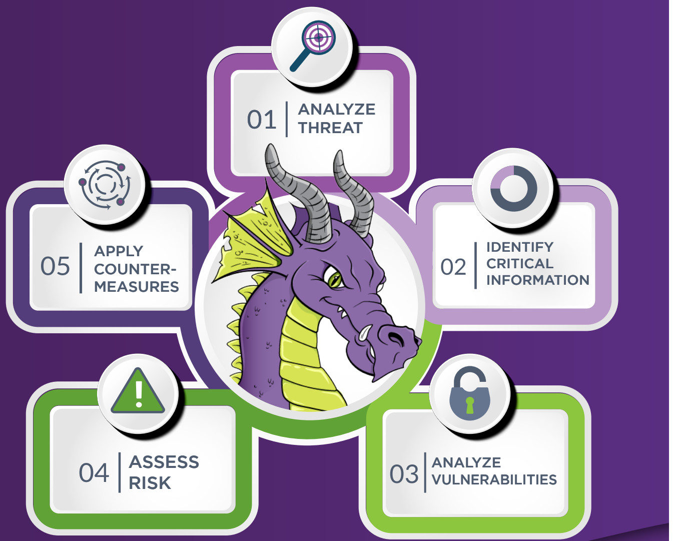
OPERATIONS SECURITY

DENY THE ADVERSARY

www.IOSS.gov

5 STEPS TO PROTECT –

Our people, information, and mission:



01 ANALYZE THREAT

02 IDENTIFY CRITICAL INFORMATION

03 ANALYZE VULNERABILITIES

04 ASSESS RISK

05 APPLY COUNTER-MEASURES

ANALYZE THREAT

THINK:

Who wants your critical information?

Is there more than one adversary?

Why does the adversary want your critical information and what is their objective?

Do they have the capability to get your critical information?

What methods or techniques can they use to get your critical information?

IDENTIFY CRITICAL INFORMATION

THINK:

What information do you need to protect?

Why do you want to protect it?

What information is of value to an adversary?

PROTECT:

Current and future operations

Travel itineraries

Operations planning information

User names and passwords

Addresses and phone lists

Budget information

Building plans

VIP/distinguished visitor schedules

ANALYZE VULNERABILITIES

THINK:

How can the adversary get your information?

How is it protected or not protected?

PROTECT:

Lack of training and awareness

Predictable patterns and procedures

Critical information posted on the internet or discarded in the trash

Non-secure communications

ASSESS RISK

THINK:

Is the risk great enough to do something about the threat?

How will the loss of critical information affect your operations?

What is the cost of losing critical information?

APPLY COUNTERMEASURES

THINK:

How can you stop the adversary from getting your critical information?

Can you use the same countermeasure(s) for many operations or do you need to develop unique countermeasures?

PROTECT:

Training and awareness

Cross shred sensitive documents

Encrypt email

Limit web page access

Use caution when having conversations in public areas

Install software patches and updates

THINK. PROTECT. OPSEC.