2017-2018 Subcontractor OPSEC Training
Government Programs

September 5, 2017

What is OPSEC and Why is it Necessary?

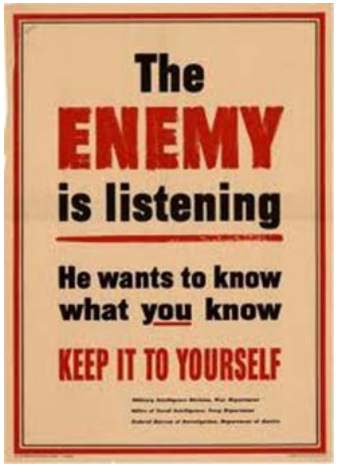
Operations Security (OPSEC): A risk management tool used to deny an adversary information concerning our activities, limitations, intentions and capabilities by identifying, controlling, and protecting indicators associated with the planning and execution of a mission.

A good understanding of OPSEC is vital to a program's success because:

- Our adversaries want the information we have
- The threat is real and is evolving with an increased level of sophistication
- The DoD and its contractors have been declared a clear target
- Practicing good OPSEC principles does more than just protect information, it also protects:
  - Soldiers
  - The Program
  - The Company
  - Your Job!

The OPSEC Process

1. Identify critical information
2. Analyze threats
3. Analyze vulnerabilities
4. Assess risks
5. Apply OPSEC countermeasures



- As you work your way through this brief, you will see that much of the work in this process has been initiated
- An OPSEC plan must be constantly reviewed, especially when looking at identifying vulnerabilities and countermeasures
- If you identify a vulnerability we aren't protected against or have a proposed countermeasure, please contact your local security staff

Threats and Adversaries

- Who Is A Threat?
  - Any individual, organization, or country that has the **intent** and the technical **capability** to attack us by exploiting our vulnerabilities

- Who Is An Adversary?
  - Anyone who may be collecting information about us and our organization and intends to use this information to defeat our operations or plan an attack against us. Examples of adversaries include:
    - International Terrorists Groups
    - Criminals
    - Anti-government Militia Groups
    - Insider threats
    - Extremist groups
    - Foreign Intelligence Agencies
    - Hackers

How Does an Adversary Gather Intelligence?

- Human Intelligence (HUMINT)
  - Recruitment
  - Blackmail
  - Requests for information
- Signal Intelligence (SIGINT)
  - Intercept communications
- Open Source Intelligence (OSINT)
  - Information available on internet
  - News releases
- Imagery Intelligence (IMINT)
- Measurement and Signature Intelligence (MASINT)
- Computer Intrusions
- Insider Threat

What Are Adversaries After?

- Short answer: Anything they can get access to
- Would like classified information but that is difficult
- Most collection efforts center on gathering unclassified information with a focus on “sensitive” information that can go by many different names
  - Critical Information
  - CUI
  - FOUO
  - Technical Data
- In order to protect this information we must first properly identify it, determine vulnerabilities and employ countermeasures to mitigate risk

Critical Information List (CIL)

- Testing information for the government programs compromising location, date, time and method of transportation for components, vehicles, and/or equipment.
- Government specific technology development activities relating to milestones, technology readiness, goals, and funding activities.
- Specific and projected system vulnerabilities that Air Methods is working to enhance vehicle survivability and sustainability. Be wary of discussing the areas of Survivability, Intelligence or Combat Improvements, Electronic Warfare, C4ISR, Mission Command upgrades.
- Air Methods information systems; electronics; lasers, optics, command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR); modeling/simulation; and sensors.

Critical Information List (continued)

- Operational readiness or specific equipment on a vehicle that is causing any operational issues of Air Methods units deployed or being deployed. If in the future wireless downloading of vehicle data is authorized, download of a single vehicle's data will be FOUO but download of entire unit's data could identify a vulnerability or limitation for combat operations.
- Photos of or information about vehicles or equipment that have been damaged by Threats. Combat damage photos of any vehicle should not be commented on, noted or discussed in open forum. No discussion of what type of IED Jammers or IED defeat systems being worked on. Any information or threat or threat comments on anything that hits and penetrates Government vehicles should not be posted on NIPR or open source.
- Specific friendly force technology areas of details, organizational initiatives, and Operational procedures designed to counter IEDs. This includes IED CONOPS, IED TTPs, IED Counter Devices, Counter IED Capabilities or Limitations, Ongoing Counter IED upgrades.

Critical Information List (continued)

- Air Methods system requirements, capabilities, threshold/objective specifications, and performance measures. This would also include future, projected or targeted capabilities.
- Identification of reliability or effectiveness, operational limitations, and vulnerabilities against ballistic, non-ballistic, nuclear, chemical, biological, and electronic warfare disclosing vulnerabilities and limitation.
- Custom computer software/unique algorithms used for the government. This includes Vetronics, Fire Control, VICTORY, Wireless capabilities and limitations, Information Assurance and Crypto requirements. Each Systems Real Time Operating Environment and Computer Language requirements.
- Identification of Critical Program Information (CPI) and Program Protection Plan (PPP) within the vehicle and associated critical functions, Program Protection procedures, and anti-tampering implementation methods.

What is Controlled Unclassified Information (CUI)?

- CUI is information that is **unclassified** but considered sensitive by the government, therefore requiring **additional protection**
  - CUI is **NOT** classified information (i.e., confidential, secret and top secret information)
  - Personnel must have a “need to know” in order to access

CUI ≠ CLASSIFIED

- The types of information considered to be CUI are
  - **For Official Use Only (FOUO)**
  - **Technical Data**

For Official Use Only Definition

- For Official Use Only (FOUO) is a government designation applied to unclassified information that may be exempt from mandatory release under the Freedom of Information Act
- Government employees are required to designate/mark information as FOUO if any of these items are true:
  - The **Security Classification Guide (SCG)** for the program identifies the content as FOUO
    - If you don't have a copy of your program's SCG, please contact your program lead
  - FOUO information is taken from an **existing document** and put in a new document
    - If there is a conflict between an existing document and the SCG, the SCG takes precedence
  - Directions in a **CDRL** state that the document must be designated as FOUO

Technical Data Definition

- Technical Data is **any recorded information** related to **experimental, developmental or engineering works** that can be used to define an engineering or manufacturing process, or can be used to design, procure, produce, support, maintain, operate, repair or overhaul program material
  - The data may be **graphic** or **pictorial** delineations in media (e.g., computer software, drawings, or photographs), **text** in specifications, related performance or design documents or computer printouts
- Examples include:
  - Research and engineering data, engineering drawings and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications and related information, and computer software documentation

The definition of technical data is very broad; much of the data used during a contract will be considered CUI

Public Domain

- What is Public Domain Information?
  - Unclassified information that does not qualify for the status of CUI and is deemed suitable to release to the public
  - All program information **must** be reviewed and approved prior to release to the public
    - Air Methods conducts an internal review
    - Final approval provided by the government
    - Please contact Security or Communications for additional information

WARNING

Just because something appears in the public domain doesn't necessarily mean that it is public domain information; we must still follow correct procedures to release all information

Vulnerabilities and Countermeasures

- Our adversaries are constantly looking to identify our vulnerabilities in order to exploit them
- A countermeasure is anything that effectively negates or reduces an adversary's ability to exploit our vulnerabilities
  - Contract defines many protection requirements
  - Company required to deploy systems that meet the requirements
- The following slides will cover countermeasures we will use to protect information
- Countermeasures only work if people use them!

Access

- CUI may be released to a Air Methods employee that is a **US Person** (e.g., US Citizen or Green Card holder) that has a "need to know" to access the information
- CUI may be provided to **US DoD subcontractors** in order to conduct official business (e.g., a subcontract) **unless** there is a Distribution Statement on the material that provides different guidance
- **Do not share CUI material with foreign entities** without first ensuring that the appropriate approvals are in place with Export and Security
- If you provide CUI material to others, **you are responsible for ensuring they know the proper handling procedures**
  - CUI handling requirements are required to be flowed down to all subcontractors/suppliers that will have access to CUI

Storage and Handling

- CUI material shall not be left out on desks or where others can get access; **lock CUI in a desk or cabinet** at night
- **Do not** process CUI on public computers (e.g., hotel business centers) or personal computers
- CUI shall not be displayed in public places such as airports, airplanes, restaurants, etc.
- Face to face meetings are good but only if held in controlled areas, meaning that others can’t see or hear what you are doing

Storage and Handling (continued)

- At no time should CUI material be stored on drives that permit access to users without the proper “need to know” (e.g., “Temp” folders on common drives)
- CUI may be stored on shared network drives (e.g., K:, O:, etc.); however, a program may direct storage in another location (e.g., EPDM)
- Only provide access to personnel with the **proper need to know**
  - Ensure onboarding process is in place within program to validate need before granting access
- **Remove access** when no longer needed
- Destroy CUI when no longer needed

Devices and Media

- **Personally owned computers/devices are NOT authorized to process or store CUI**
- Portable electronic devices (e.g., smartphones, laptops, tablets) and removable media (e.g., external hard drives, USB drives**) must be physically and electronically protected** using NIST/NIAP approved encryption
- Optical Media (e.g., DVDs and CD's) requires physical protection but does not require encryption
- If travelling with a company device such as your **laptop**, you are not permitted to check it in your luggage; **you must carry it on the plane**

Transmissions

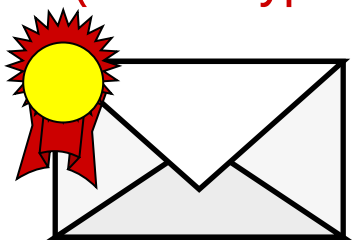
- CUI may be sent through mail channels, commercial carrier (e.g., FedEx) or hand-carried
- Landline communications for telephone conversations are more secure but it is permissible to use cell phones
- Transmit voice and fax only when authorized recipients will have access to the transmission
- You **may** transmit CUI within the company network without additional protection/encryption
- **CUI that leaves our company network is required to be encrypted using NIST/NIAP approved encryption**

E-mail

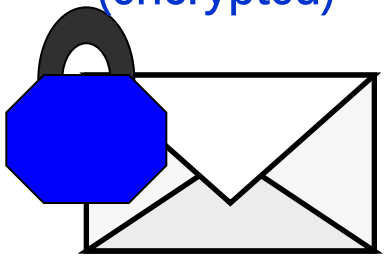
- Internal Email (within company network): you **MAY** transmit CUI data within the US domain without any additional protection

- External Email (outside of company network): you **MAY NOT** transmit CUI unless there is appropriate encryption (PKI certificates)

DIGITAL SIGNATURE
CONFIRMS WHO SENT MESSAGE
(not encrypted)



ENCRYPTION
UNINTELLIGIBLE TRANSMISSION
(encrypted)



- **NEVER** use commercial e-mail accounts (e.g., Yahoo, gmail, hotmail, etc.) or file hosting services (e.g. Dropbox, Google Drive, etc.) for business purposes

External Transmissions

- **Secure File Transfer Service (SFTS)** is a tool that will allow you to share CUI material with others
- **AMRDEC Safe File Exchange (SAFE)** is a government application and approved for transmission of CUI
- Air Methods EPDM is approved for the transmission of CUI

Web Meetings

- **WebEx is an approved method** to both discuss and display CUI material
- **MS Online / Lync / Air Methods version of Skype (all internal)** meeting is an approved method for meetings
- **Defense Collaboration Services (DCS)** is a government system similar to WebEx and is an approved system for sharing CUI information
- Other third party applications such as Skype (w/external connection), FaceTime or Go To Meeting are not approved at this time

VPN and Smartphones

- Smartphones
  - Employees are NOT permitted to transmit CUI via text message, iMessage, Blackberry Messenger (BBM) or similar service
  - The use of the camera/video function on Smartphones or Tablets **is prohibited**

Markings

- Appropriately marked CUI documents are vital to the protection of the information included in the document
- If you create a document with CUI, you are required to mark it appropriately
- In order to know exactly what CUI markings are needed, you will need access to the program SCG, the applicable CDRL and/or a properly marked source document

Markings (continued)

- Technical Data Markings
  - All material containing technical data must have a Distribution Statement placed on the front cover or first page of the document
- FOUO Markings
  - All unclassified materials containing FOUO information will be marked “FOR OFFICIAL USE ONLY” in letters larger than the rest of the text, where practical, at the bottom of the front cover, the title page, or the first page, and the outside of the back cover
  - Pages within the document which contain FOUO information will be marked “FOR OFFICIAL USE ONLY” at the bottom

Visit Control

- Visitors are required to process through established checkpoints prior to access to the facility
- Escorts for visitors are responsible to know
  - Proper escort procedures
  - Limitation on disclosure
  - Any other applicable controls involved in the visit
- All foreign visitors must be approved in advance by Export Control and Security
  - All licenses and government approvals must be in place prior to sharing any program information with a foreign national or a person representing a foreign company

Violations

- Violations of the CUI requirements can take on many different forms:
  - Improper storage of CUI
  - Providing a person without a need access to CUI
  - Discussing CUI in a public place
  - Discussing CUI on social media
- **The number one violation is the use of unapproved transmission methods**
- If you recognize a violation, you are required to notify the author/sender and Security about the issue
  - It is necessary to identify and correct issues quickly in order to stop the spread of the violation

Practice Good OPSEC!

- Don’t talk about work outside of work
  - This applies to discussions with your family as well
  - Adhere to the Air Methods Social Media Policy
- When you travel or are outside the facility, don’t broadcast who you work for or what program you are working on
- Contact Security prior to any foreign travel to get the appropriate briefings
- Be aware of unusual or social contacts that want to know about the work that you do. **Report these instances to Security ASAP**
- Practice good “need to know” principles

QUESTIONS?

Contact your local security department for any assistance that you may need.

1.1 Critical Information List

- Testing information for government programs compromising location, date, time and method of transportation for components, vehicles, and/or equipment.
- Air Methods specific technology development activities relating to milestones, technology readiness, goals, and funding activities.
- Air Methods system requirements, capabilities, threshold/objective specifications, and performance measures. This would also include future, projected or targeted capabilities.
- Identification of reliability or effectiveness, operational limitations, and vulnerabilities against ballistic, non-ballistic, nuclear, chemical, biological, and electronic warfare disclosing vulnerabilities and limitations.

Critical Information List (1 of 3)

- When, where and how often specific groups/teams/pairs of Air Methods employees travel for government business, i.e., Intelligence Electronics Testing, Worldwide Armor Conference, C4ISR Conference, etc.
- Specific and projected system vulnerabilities Air Methods is working on enhancing vehicle survivability and sustainability. Be wary of announcing what specific areas on Survivability, Intelligence or Combat Improvements, Electronic Warfare, C4ISR, Mission Command upgrades.
- Custom Computer software used in government weapons system development, testing and evaluation. This includes Vetronics, Fire Control, VICTORY, Wireless capabilities and limitations, Information Assurance and Crypto requirements. Each Systems Real Time Operating Environment and Computer language requirements.
- Information Technology architecture and SharePoint portal system vulnerabilities.

Critical Information List (2 of 3)

- Identification of Critical Program Information (CPI) and Program Protection Plan (PPP) Implementation methods - Location of CPI within the weapon system; identification of contractor Developing CPI; protection measures implemented to protect CPI and critical functions of the weapon system.
- Operational readiness or specific equipment on a vehicle that is causing any operational issues of AMPV units deployed or being deployed. If in the future wireless downloading of vehicle data is authorized, download of a single vehicle's data will be FOUO but download of entire unit's data could identify a vulnerability or limitation for combat operations.
- Photos of or information about vehicles or equipment that have been damaged by Threats. Combat damage photos of any vehicle should not be commented on, noted or discussed in open forum. No discussion of what type of IED Jammers or IED defeat systems being worked on. Any information or threat comments on anything that hits and penetrates our vehicles should not be posted on NIPR or open source.

Critical Information List (3 of 3)

- Specific friendly force technology areas of details, organizational initiatives, and Operational procedures designed to counter IEDs. This includes IED CONOPS, IED TTPs, IED Counter Devices, Counter IED Capabilities or Limitations, Ongoing Counter IED upgrades.
- Technological, organizational, or operational capabilities. This would also include future, projected or targeted capabilities.
- Classification levels of the program - Special Compartmented Information (SCI) and Special Access Program (SAP) access; Security Classification Guide (SCG) identifies classified Critical Information; Department of Defense (DD Form 254), if addressing SCI or SAP.