Operations Security (OPSEC) Training for Aerojet Rocketdyne Suppliers

October 30, 2018

Presenter: SCMM Compliance

Training Introduction

This training is part of continuing efforts to provide security education and awareness through web-based training and may be a requirement of customer contracts. Suppliers who use this training are required to maintain records of employee completion that shall be available for inspection upon request by AR and its customers.

The Importance of OPSEC

- **Protecting critical and sensitive information is essential to ensuring the success of the company and our mission, and protecting the lives of U.S. Service members, Department of Defense employees, Contractors and family members**

The Purple Dragon

- The year was 1967, the height of the Vietnam War. National leadership became concerned that our B-52 Bombers were being shot down at a very high rate. It was apparent that the North Vietnamese had been gaining prior knowledge of our bombing mission times and locations.
- ***Operation Purple Dragon was born.*** It was designed to analyze our military operations from the adversary's perspective.
- Amazingly enough, we discovered that procedures established before the war required pilots to file their flight plans with civilian air controllers in Manila. These plans were then sent out over International Air Traffic Control Channels. Our bombing mission flight plans were being received directly by Hanoi!
- OPSEC has been used many times in warfare throughout the centuries. As OPSEC has developed into a system of analyzing threats and employing countermeasures, the Purple Dragon symbol has come to represent the adversary that we must be on guard against at all times. ***Today, when you see the Purple Dragon symbol, we hope you'll "Think OPSEC."***

What is OPSEC?

OPSEC Is:

- A Process, Not A Set of Rules
- A Method for Denying an Adversary Access to Our Critical Information
- Part of Everyone's Job – Including Yours!

A Five Step Process:

1. Identify Critical Information
2. Analyze Threats
3. Analyze Vulnerabilities
4. Assess Risks
5. Apply OPSEC Countermeasures

Identify Critical Information

Critical Information Includes:

- Information About Business Activities, Intentions, Capabilities, and Limitations
- Information Relating to Military Technologies, Vulnerabilities, and Performance Data
- Personal Information About People You Work With
- Any Information That Is Useful to An Adversary

Indicators Point to Critical Information or Vulnerabilities. *They're Like Pieces of a Puzzle an Adversary Uses to Reveal a Picture of Our Operations.*

Indicators include:

- Words, Phrases, or Actions That Draw Attention to Critical Information
- Unusual Activity or Changes in Routine
- Clues an Adversary Can Interpret to Uncover Hidden Information

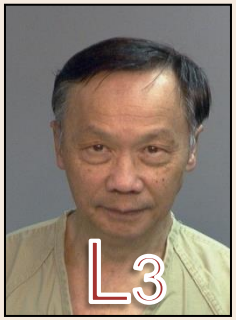
Analyze Threats

Who Is An Adversary:

- An Individual, Group, Organization, or Government That Must be Denied Critical Information
- Not Necessarily a Sworn Enemy, Foreign Government, or Military Power
- Any Person or Group Whose Intentions and Capabilities Are Contrary to Ours

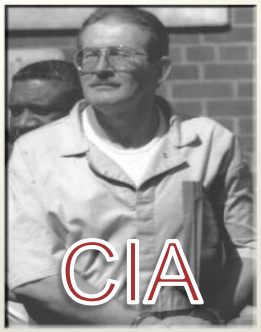
The Insider Threat Is Real!

Chi Mak



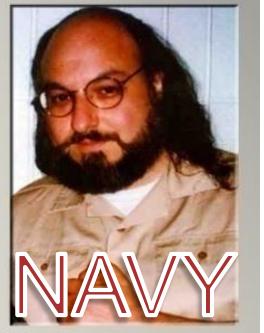
26 Years

Aldrich H. Ames



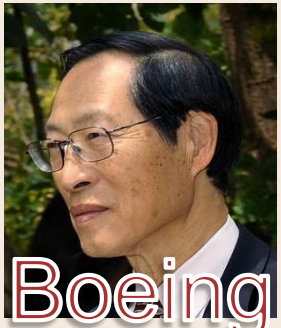
Life without parole

Jonathan J. Pollard



Life

Dongfan "Greg" Chung



15 Years

Analyze Threats

Insider Threat Reportable Indicators:

- Attempts to Obtain Info Without a Genuine “Need to Know”
- Repeated or Unusual or Unnecessary Overtime
- Unauthorized Removal of Classified, Sensitive, or Proprietary Info
- Repeated Attempts to Bring Electronic Devices Into Sensitive Areas
- Excessive Hoarding of Sensitive Information
- Sudden Purchase of High-Value Items That Income Does Not Match
- Extensive or Regular Gambling Losses or Financial Indebtedness
- Upon Return From Travel, Employee Has Difficult Time Describing Travel Details; Avoids Questions
- Sudden Changes in Demeanor, i.e., Disgruntled, Depressed, Angry, Moody, Temperamental, Sad, Isolated and/or Defeatist

*** Remember: Observe and Report. Do Not Directly Confront Employee!**

Analyze Vulnerabilities

A Vulnerability Exist When An Adversary Can:

- Exploit Weaknesses to Obtain Critical Information
- Take Timely Action Against Our Business Based on That Information

Vulnerability Examples:

- Discussions and Phone Calls in Public Places
- Telephone and Cell Calls, and E-Mails That Can be Intercepted
- Social Networking Sites, Blogs, and Other Postings on the Internet
- Printed or Written Information That Can Be Removed From The Trash
- Disclosing Too Much Information to Family and Friends
- Unauthorized Disclosure of Official Information to the Press
- One of the Most Common Vulnerabilities is *Simply Talking Too Much*

Assess Risks

Threat x Vulnerabilities x Impact = Risk:

- Consider the Consequences of Your Actions
- Will Something You Do or Say Provide an Indicator to An Adversary?
- What's the Effect on Business/Programs?
- What Is the Cost of Avoiding the Risk?

For Official Use Only (FOUO) Information

- Program Material Identified as “For Official Use Only” (FOUO) must be handled to preclude its disclosure to the general public and to limit its circulation based on “need-to-know”
- FOUO Material can be stored in unlocked files, desks or similar containers if the office or building is locked after business hours; if the building or office is not locked after business hours, FOUO must be stored in locked rooms, desks, bookcases or file cabinets; FOUO material must not be left unattended when removed from storage —put it in a drawer out of sight when leaving your work area even for a short time; FOUO material should be wrapped (single) and sealed if being hand-carried between facilities
- The marking “For Official Use Only” must be stamped or marked in bold letters near the bottom on the outside front cover, on the first page, and on outside back cover (if any). For convenience, all pages, even those that do not contain FOUO information, may be marked “for official use only” in documents generated through automation; FOUO, in abbreviated form, can NOT be used as a page marking

Remember to Properly Secure It Before Leaving for the Day

The Pizza Story

DESERT STORM SCENARIO

- **OPSEC INDICATORS:**

  400 Domino's Pizzas delivered to the Pentagon

  +

  Numerous vehicles in Pentagon Parking Lots after duty hours

  ---

  = Start of Ground Invasion of Kuwait

Apply OPSEC Countermeasures

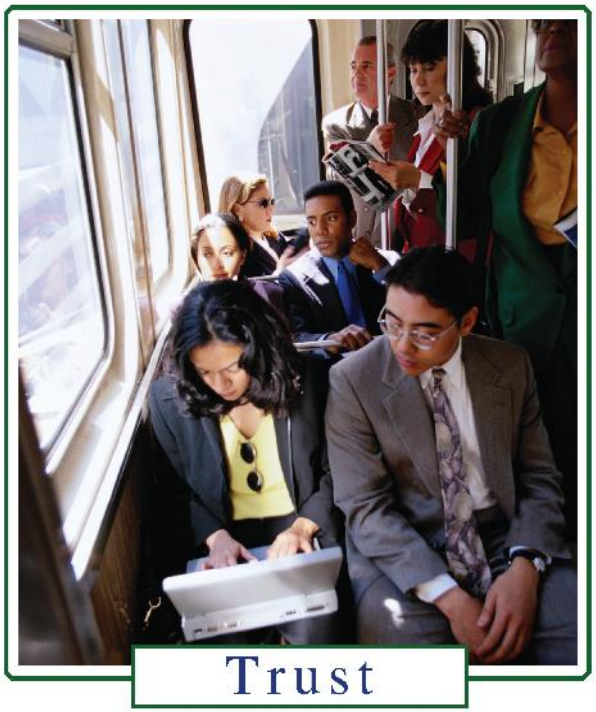
- Conceal Indicators That May Point to Critical Information or Vulnerabilities
- Make Indicators Seem Unimportant
- May Be As Simple as Choosing Not To Talk About Something
- Protect Critical Information
- Do Not Display Credentials (ID Badges) In Public Places
- Set Up Password Protection on Social Networking Web Sites
- Avoid Discussing Your or Other Employee's Business Travel Plans
- Conceal Indicators by Looking for a Private Location During Business Phone Calls
- Avoid Divulging Indicators by E-Mail, Especially External E-Mail
- Refer All Public Media Inquires to the Communications Department

Critical Information Protection Steps

- Disclose Business/Program Information Judiciously; Need-To-Know
  - The Possessor of the Critical Information is The Release Authority
  - An OPSEC indicator could be Business Development projects, financial transactions, motor movements, or Emergency Response Drills. Before releasing the information consider the potential value to your adversaries and competitors.
  - The loss of the government's unique intellectual information can be priceless to an adversary or business competitor.

Countermeasure Practical Application

- Do Not Discuss Your Work in Public Places or Where Others Can Overhear Your Conversation
  - Avoid “Shop Talk”.
    - Shop Talk is conversation about matters pertaining to a person’s occupation often conducted outside of work areas and working hours, as in social gatherings.
  - Family and friends *do not* have a Need-to-Know
  - Discussions outside of approved areas or with individuals without a Need-to-Know may constitute an unauthorized disclosure.



Protect the information you are entrusted with;
You never know who may be looking over your shoulder.

Countermeasure Practical Application

- Do Not Discuss Critical Information on Unencrypted Telephones
  - Secure Terminal Equipment (STE) should be used in the encrypted mode when discussing FOR OFFICIAL USE ONLY (FOUO) information over the phone.
  - A secure FAX machine (connected to a STE) in the encrypted mode should be used to transmit FOUO.
- Protect Mass Media Devices Containing Critical Information
  - Use of USB storage devices or other external storage devices may be easily hacked; contractors shall ensure that employees are familiar with their policies.
  - Thumb drives are popular but risky. Contractors should consider limiting use to only approved thumb drives and establishing password protections. Prohibit use of trade show thumb drives on networked devices.
  - If lost or stolen notify security/export control immediately.

Personal Electronic Devices (PED)

- **Suppliers shall establish appropriate policies regarding use of PEDs consistent with regulatory requirements (DFARS/NIST) and ensure that employees are aware of all requirements.**
- **Training on Cyber Awareness (Information Assurance) Computer Based Training (CBT) module which meets federal requirements shall be provided to all employees.**
- **Evidence of completion of training to be documented and retained for at least one year.**

Countermeasure Practical Application

- **All AR proprietary, customer sensitive (CUI, FOUO) and/or International Trafficking in Arms (ITAR)/Export Administration Regulations (EAR) data must be encrypted either using Sophos or digital certificate.**
- **Alternate: To provide information to Aerojet Rocketdyne, use iCollab or Aeroframe**

Countermeasure Practical Application

- Do Not Reveal Critical Information, Indicators, or Personal Information on the Internet
  - The enemy is:
    - ✓ Following Tweets
    - ✓ Connected to Social Media
    - ✓ Sending “Phishing” E-Mails
    - ✓ Monitoring Chat Rooms and Forums
- When you post information to the net, via your blog, MySpace, e-mail, etc., you have to assume that it’s going to be there forever.
- The only safe bet is to make sure it never gets there.

Countermeasure Practical Application

- Shred Paper Documents Before Placing Them in the Trash
  - All program and proprietary documents must be destroyed to prevent reconstruction.
  - The minimum standard must be met:
    - ✓ Cross Cut Shredder with a maximum width of ¼" and maximum length of 1 ½"
- Unclassified business information may be placed in company shred barrels to be destroyed.
- Information on Hard Drives Will Be Sanitized per the Industrial Security Field Operations (ISFO) manual.
- CD's and DVD's Will Meet the Same Minimum Standard as Paper Documents.

Countermeasure Practical Application

- Refer All Inquiries From The Press to Aerojet Rocketdyne Communications Department via the Buyer
  - Any information (classified or unclassified) pertaining to a contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted to Aerojet Rocketdyne for approval prior to release.
    - Required for Unclassified & Classified Programs
    - Material is NOT Automatically Approved for Public Release Just Because it is Unclassified.
    - Government Customer is the Final Approver

Data Spills

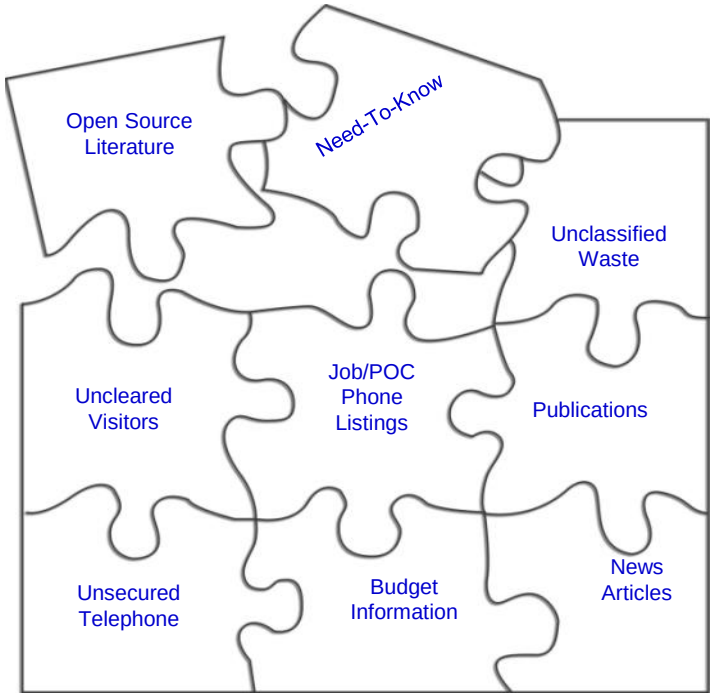
- In the event that there is a data spill, suppliers shall immediately notify Aerojet Rocketdyne.

- Suppliers shall retain information about data spills and share “lessons learned” in regular employee awareness sessions.

Operations Security (OPSEC)

- **OPSEC…Is Everyone's Responsibility!**

  Without your continued support, all the hard work and money spent on our programs could be for naught. The threat is real and you must help thwart it!



That One Piece of Harmless Information You Unwittingly Give Away Could Be the Piece That "Completes the Puzzle"

Congratulations

You have completed this presentation!

Please complete a class roster to record training and retain it for inspection.