

Operations Security (OPSEC)



Sandia National Laboratories

2011 FSO Conference

“Protecting Corporate, Company, and National Interests”

Matt Umstead
SNL OPSEC Program Manager



Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

SAND: 2011-5431C

Introduction

- Description
- Personal OPSEC
 - Think!
 - Assess!
 - Protect!



- What else?
- OPSEC practices
- ‘Killing with Keyboards’

OPSEC Description



“Security measures that control vulnerabilities to sensitive information or activities”

- Non-traditional.....designed to prevent adversaries from accessing information.
- Addresses “INADVERTENT RELEASE” of information.

Think! Assess! Protect!



Personal OPSEC

DO YOU:

- ...give out your SSN freely?
- ...share your address with strangers?
- ...handily give your credit card to simple acquaintances?
- ...double back to make sure your garage door is closed?
- ...watch your kids closely in the park?



Think!

Assess!

Protect!



- What are you protecting?
 - Is it classified? Sensitive unclassified? Proprietary?
- What threats exist?
 - Foreign Spies? Criminals? Industrial Spies? Insiders?



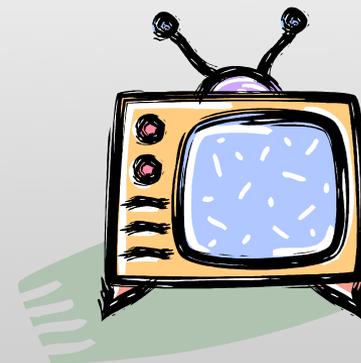
Think!

Assess!

Protect!



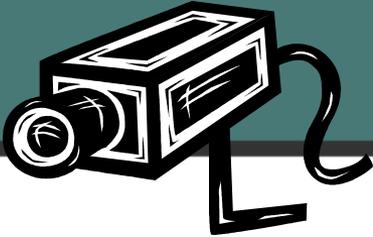
- What are the vulnerabilities to info loss?
 - Must be determined. Test your protections.
- What are the risks or consequences to loss?
 - Company interests, national interests, media, legal, reputation, loss of work, etc.



Think!

Assess!

Protect!



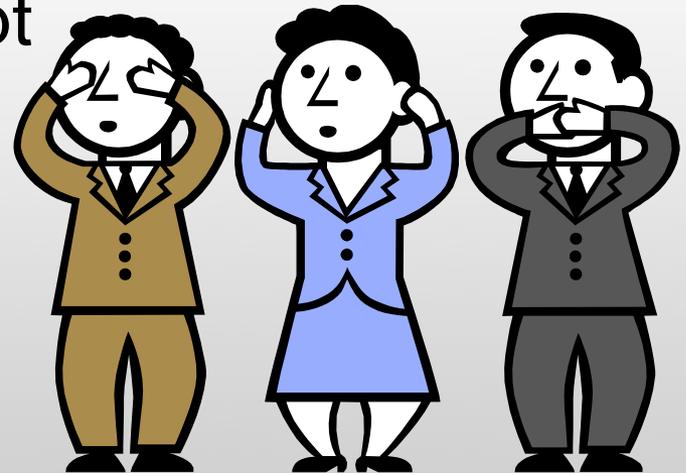
- What security measures can be applied?
 - Explore options (i.e., access, cyber, handling, destruction, etc.)
 - Cost effectiveness
- What currently exists?
 - Take credit for what you practice





What else?

- Minimize flags to sensitive information/activities
- Flags are indicators to an adversary that can create a pathway to greater sensitive info
 - Pieces of the puzzle
- Apply Need-to-Know concept



Good OPSEC Practices



- Guard information:
 - Phone, fax, and radio
 - Visual (open, cameras, sky)
 - Computer (e-mail, web, encryption, permissions)
 - Social environments (restaurants, conferences, parties)
- Careful posting on walls/bulletin boards
- Consider destruction methods (shredding, burning)
- Be aware of surroundings....report suspicious activity
- Watch vulnerabilities (trash/recycle, phone, email, web, etc.)

“Killing With Keyboards”



OPSEC Handout in Folders!

- Dangers of online social networking.
- How foreign intelligence can be collected
- Keep online awareness!
- Importance of site security settings

Group Exercise

One Man's Trash *"Dumpster Diving"*

- THINK!
 - What is sensitive?
 - Work or personal items?
 - Are there threats?
- ASSESS!
 - What is vulnerable?
 - Are there risks to loss?
- PROTECT!
 - What measures will protect the data?

