Command Indoctrination
Operations Security
(OPSEC)

ISIC
LOGO

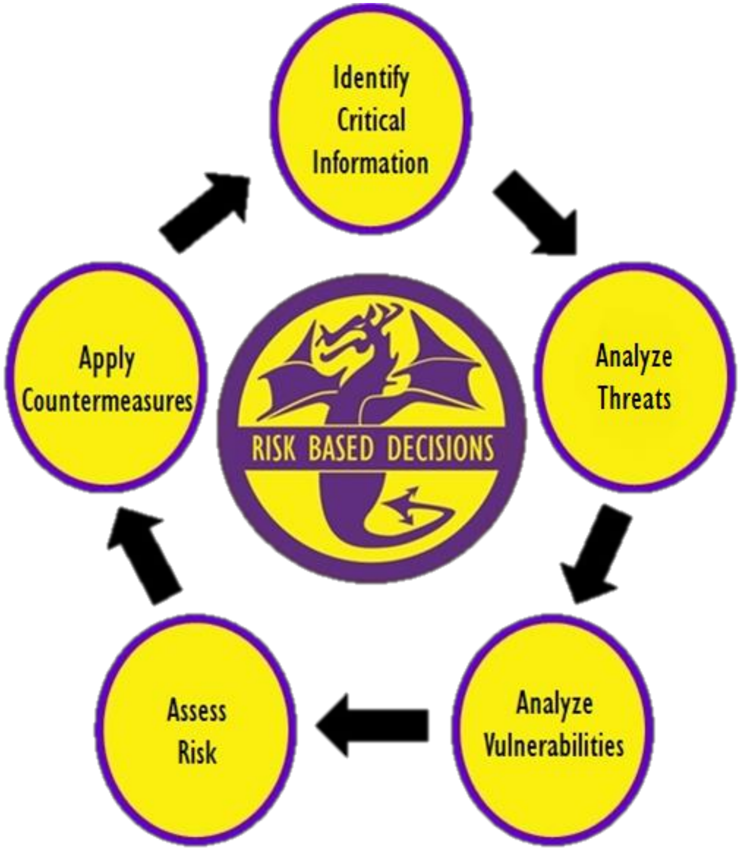
CMD
LOGO

Operations Security

- Operations Security (OPSEC) is a process that identifies unclassified critical information (CI), outlines potential threats and the risks associated and develops countermeasures to safeguard critical information.

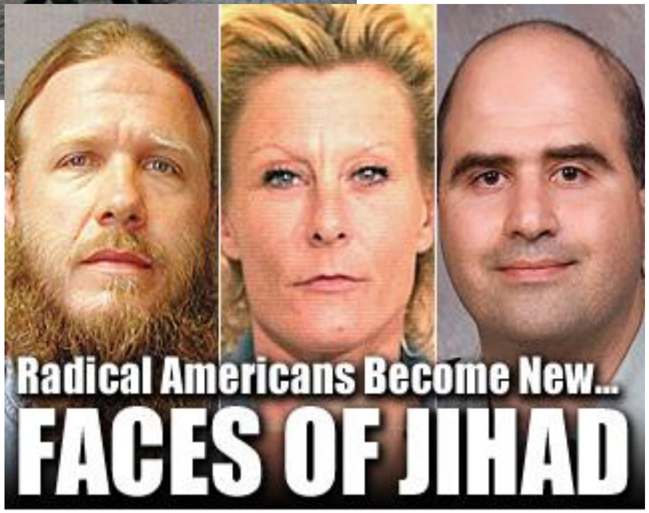
- Success of operations depends on protection of CI.

- **A 5 step process that …**
  - Identifies, controls and protects sensitive, critical unclassified information about a mission, operation or activity
  - Assesses potential threats, vulnerabilities, and risk
  - Utilizes countermeasures to mitigate an adversary's effectiveness against a friendly operation



Threat

- **Capabilities and intentions of an adversary to undertake any action detrimental to the success of friendly activities or operations.**
  - ➢ Conventional Threats
    - Military opponents
  - ➢ Unconventional Threats
    - Terrorism (foreign and domestic)
    - Hackers
    - Insiders (Spies)
    - Thieves, stalkers, pedophiles



ISIC LOGO

CMD LOGO

What are they looking for?

- **Names, photographs of important people**
- **Present/future operations**
- **Information about military facilities:**
  - Location
  - Number of personnel
  - Ammo depot locations
  - Dates and times of operations
- **Family details**
  - Spouse, children
  - Location of work, school

WATCH WHAT YOU SAY IN PUBLIC!
You never know who might be listening!
PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!

Critical Information

- **Information we must protect to ensure success**
- **Information the adversary needs to prevent our success**
  - Capabilities
  - Operations
  - Personnel
  - Security procedures

PROTECT YOUR PHONE AND LOCK IT!
Enter Passcode
Practice proper OPSEC everyday!
PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!

Personal Critical Information

- **Some examples of critical information that apply to your family life:**
  - Names and photos of you and your children
  - Usernames and passwords
  - Length and location of spouse’s deployment
  - Social Security Numbers
  - Credit card/banking information
  - Significant dates (birthdays, anniversaries)
  - Addresses and phone numbers
  - Everyday schedules
  - Travel itineraries

THESE DO ME NO GOOD OUT HERE!
Keep credit cards and important documents in a safe!
PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!

Indicators

- **Friendly, detectable actions that reveal critical information and vulnerabilities**
  - Longer working hours
  - Rehearsals
  - Sudden changes in procedures
  - Onloads
  - Large troop movements
  - Emblems/logos
  - Routine predictable procedures

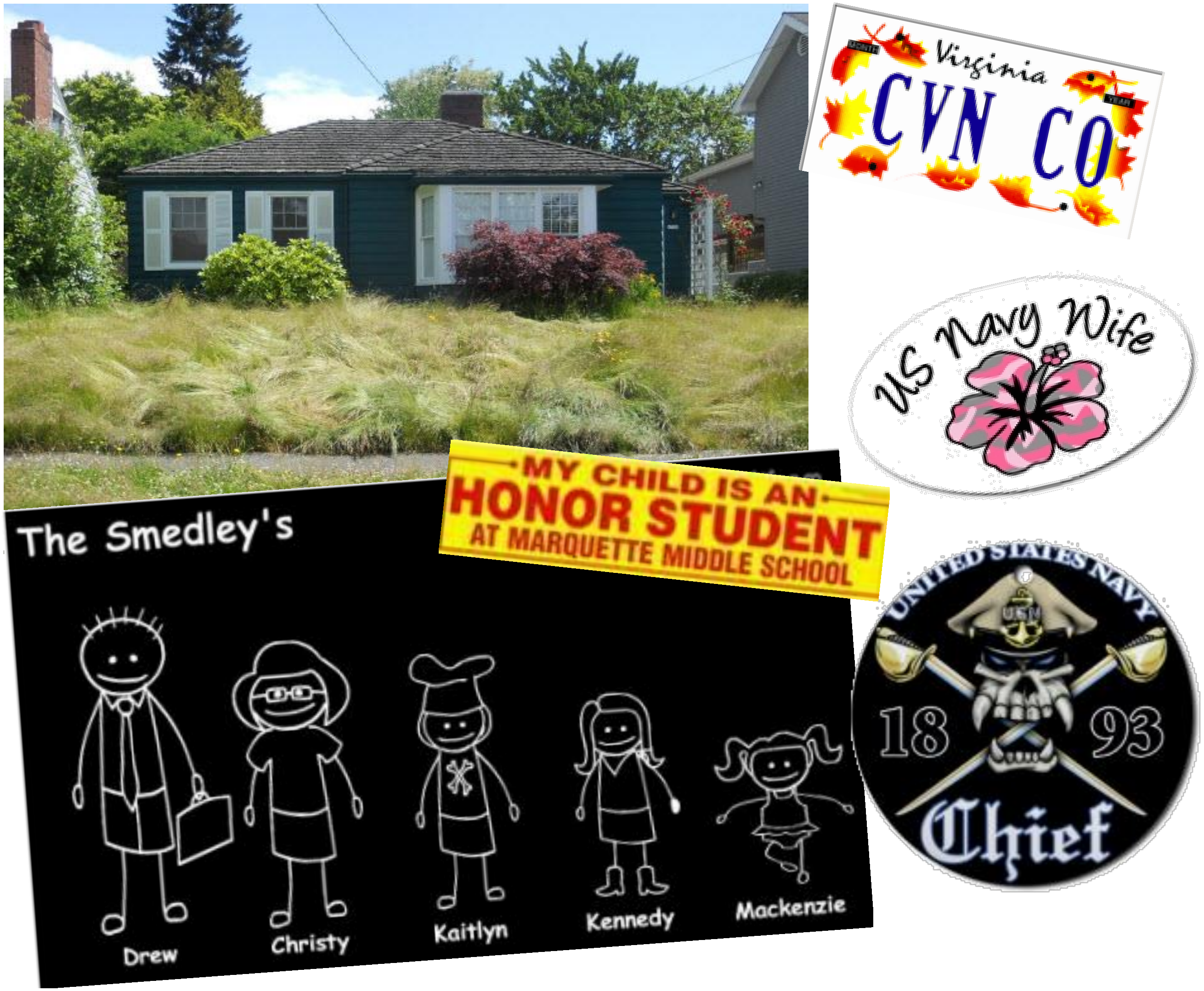
- **Not all indicators are bad**

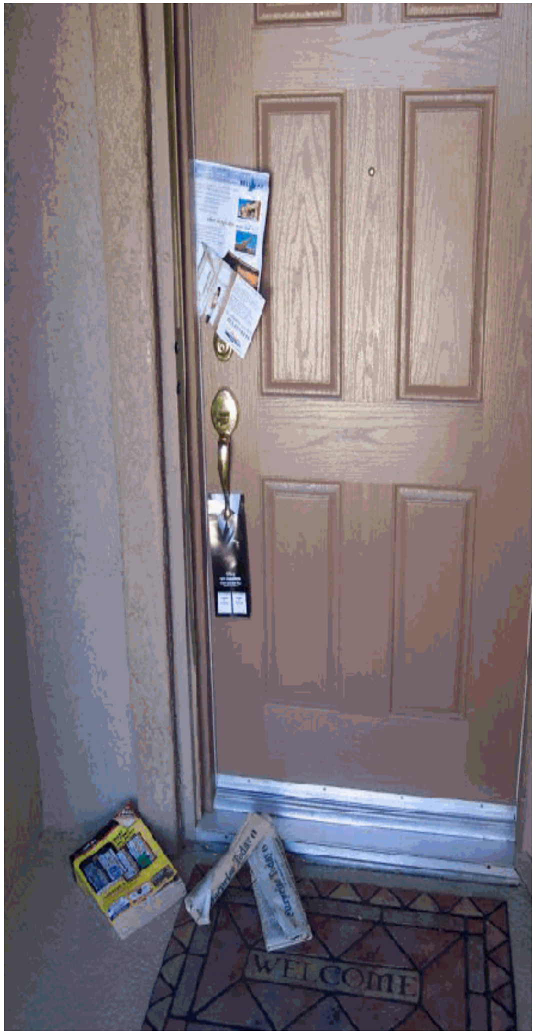
PROTECTED BY
ADT
SECURITY SYSTEMS

ISIC LOGO

CMD LOGO

Avoid Indicators





Data Aggregation

- **Information collection from multiple sources**
- **Open source collection provides enemy most of their intelligence**
- **Manchester Document: 80% of information collected is done so legally**
  - Internet
  - Trash
  - Media
- **Small details put together give big picture**

DO YOU KNOW WHAT NEEDS TO BE SHREDDED?
I bet the enemy knows!
TOP SECRET
PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!

ISIC LOGO

CMD LOGO

Vulnerabilities

- **Weakness the adversary can exploit to get CI**
- **Some common vulnerabilities are:**
  - Lack of awareness
  - Social media
  - Social engineering
  - Data aggregation
  - Technology
  - Trash
  - Poor policy enforcement
  - Unsecure communications
  - Predictable actions/patterns

SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

CAREFUL ABOUT THAT FRIEND REQUEST!
1
They might be working for the enemy!
PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!

Risk

- **The probability an adversary will gain knowledge of your CI and the impact if they are successful**
- **Impact: How much will it cost if your CI is lost?**
  - Lives
  - Mission
  - Money
  - Time

THINK BEFORE YOU POST!
Somebody could be watching!
Insta
PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!

- **How much are you willing to risk by displaying this indicator or not correcting that vulnerability?**

Countermeasures

- **Anything that effectively negates or reduces an adversary's ability to exploit vulnerabilities or collect & process critical information**
  - Hide/control indicators
  - Vary routes
  - Modify everyday schedules
- **Influence or manipulate an adversary’s perception**
  - Take no action
  - React too late
  - Take the wrong action

ISIC
LOGO

CMD
LOGO

Command OPSEC Team

- **OPSEC Program Manager (PM):**
- **Assistant OPSEC PM:**
  - **Working Group Members**

Public Affairs:

Web Master:

N1: (Name)

N2: (Name)

N3: (Name)

N4: (Name)

N5: (Name)

N6: (Name)

N7: (Name)

N8: (Name)

N9: (Name)

ISIC LOGO

CMD LOGO

Need to know

- **CMDINST 3432.1A OPSEC**
- **Command Critical Information:**
  - Capabilities / Limitations
  - Current Operations
  - ETC.
- **Realistic Threat**

Summary

- **OPSEC five step process**
- **Command OPSEC Team**
- **Command Instruction**
- **Command Critical Information**

ISIC
LOGO

CMD
LOGO

Questions