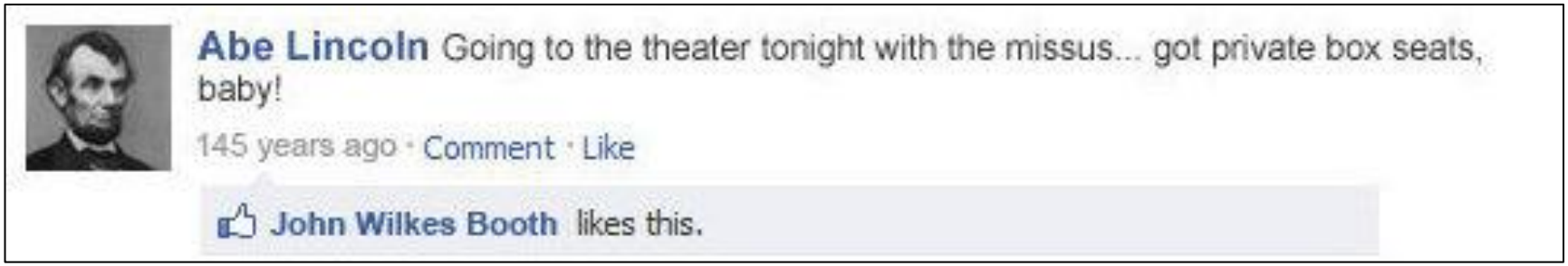
NEW YORK NATIONAL GUARD FAMILY PROGRAMS

Offered & presented by CW2 Scott Walker
Family Programs OPSEC Program Manager

OPSEC is…

- Denying any useful information to the enemy



- A mindset, a way of thinking
- Applied to web pages, blogs, emails
- A standard that can be applied to any situation

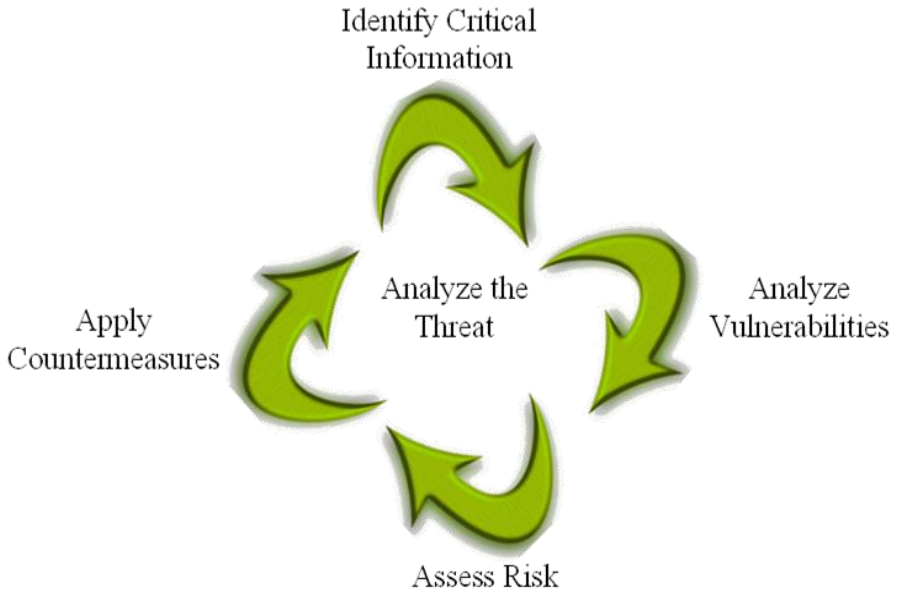
Enemies want our information, and they're not just after the military member to get it….

They also want your family members.

What Does That Mean To Us?

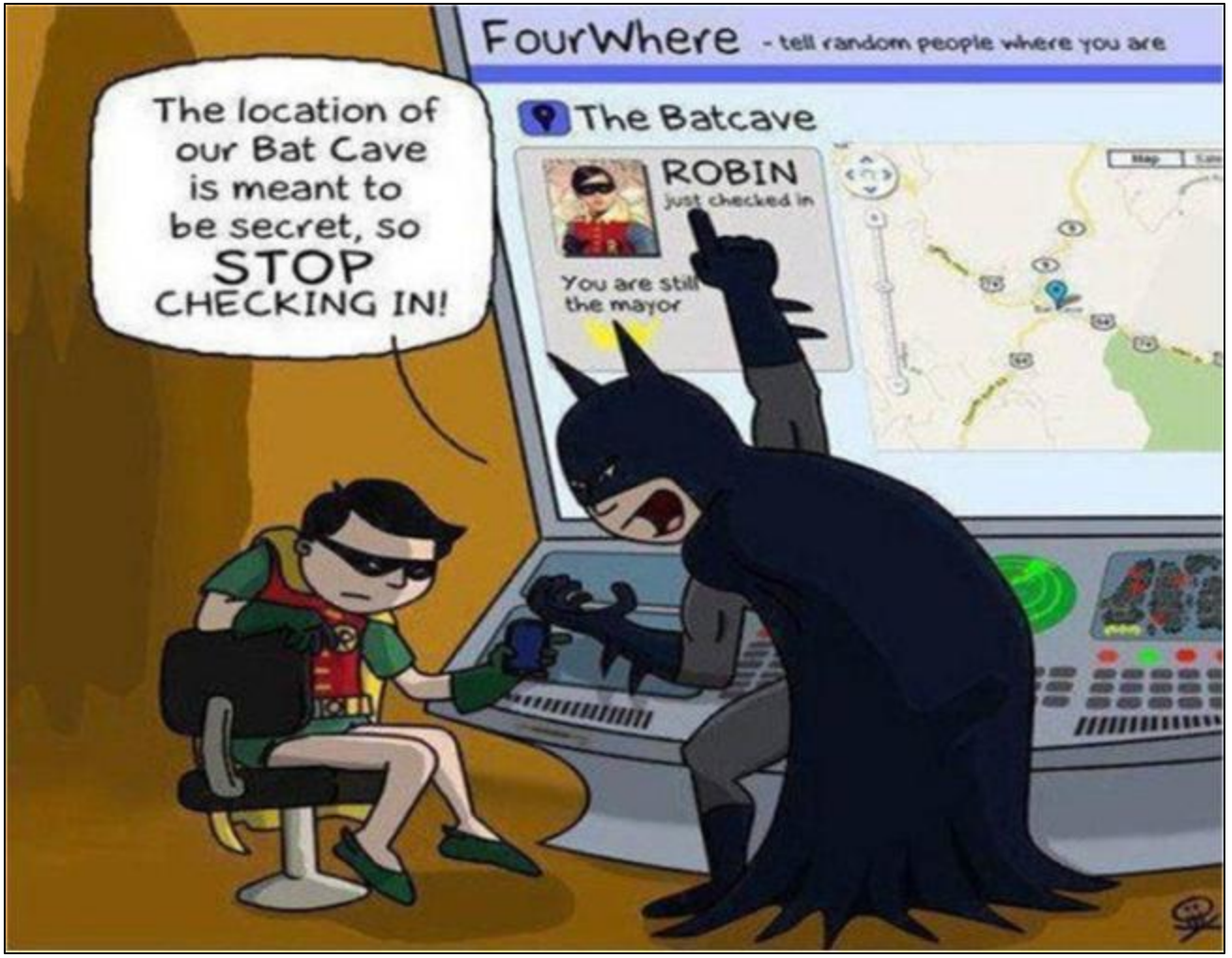
- OPSEC is practiced through the use of an OPSEC SOP or plan.
- The plan is created by following:

The 5-Step OPSEC Process



OPSEC teaches you to…

- Look
- Understand
- Assess
- Develop



Data Collection

- Information collection from multiple sources
- Al Qaeda handbook: open and legal public sources accounts for 80% of all information collected
- Legal and illegal collection methods

7.5 million young children lie about their age

Critical Information

- Information adversaries, or *potential* adversaries, need to prevent our success.
- Information we must protect to ensure success.
- Sensitive, but unclassified; (FOUO)

Critical Information

Examples:

- Personally Identifiable Information (PII): SSNs, home phone numbers, addresses, account numbers, etc.
- Locations of training exercises
- Specific details about drill weekends (exact locations, equipment, training plans, personnel involved, etc.)

Critical Information

Critical Information List (CIL)

- List of the types of critical information a unit commander has identified that require safeguarding

Critical Information

JFHQ-NY Critical Information List:

- Unit Inactive Duty Training (IDT), Annual Training (AT) periods, or work schedules.
- Mission Essential Vulnerable Area (MEVAs)
  - Protected areas which consist of information, equipment, property, and facilities
- Personal Identifying Information (PII)
- Deployment Information
- Capabilities, Limitations, and Mission Readiness of JFHQ-NY forces and equipment

Critical Information

JFHQ-NY Critical Information List:

- Security
- Intrusions Detection System (IDS) and other communication failures
- Itineraries or schedules of high risk personnel and senior leadership
- Family Readiness Group, Public Affairs, Recruiting, or any related public information release
- Lost Passwords, Combinations, or Common Access Cards (CAC) an/or Pin

Potential Vulnerabilities

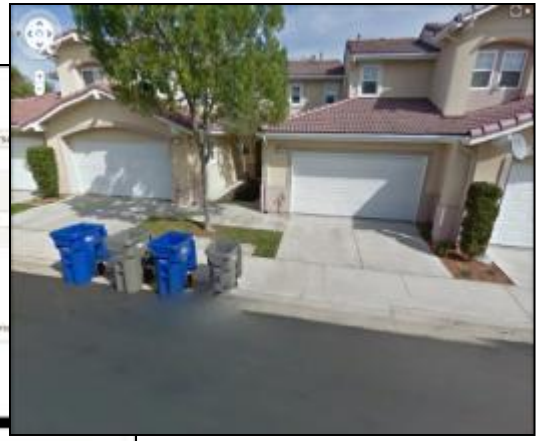
Methods used to obtain Critical Information:

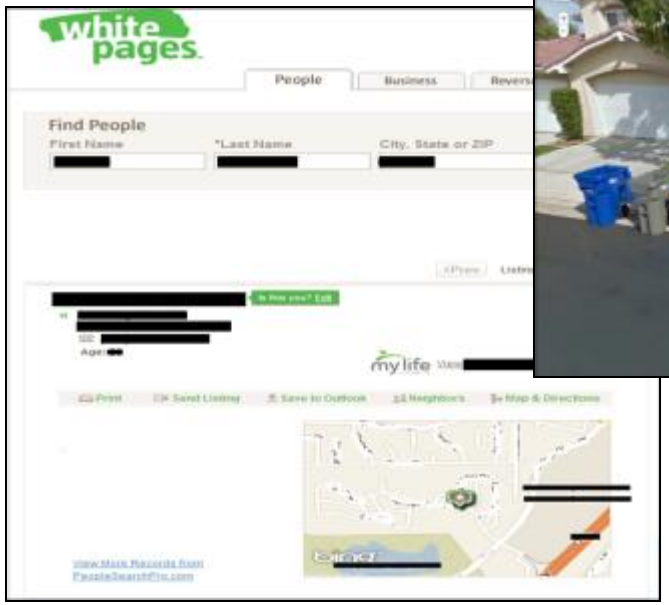
- Unprotected communications
- Sharing too much with people you don't know well
- Technology
- Trash
- Media
- Email
- Web pages
- Social Networking Sites

Illegal methods are OK with adversaries!!!


© PA


© PA




white pages
People
Business
Find People
First Name
*Last Name
City, State or ZIP
mylife

The Danger…

Bad guys use it, too:

- Stalkers
- Thieves
- Terrorist
- Hackers
- Phishers/Scammers
- Enemy organizations
- Pedophiles
- And the list goes on…

OPSEC Measures

JFHQ-NY OPSEC Measures:

- Do Not Discuss information covered in the CIL openly in public areas outside of the unit or with personnel not directly involved with the units mission.
- Shred all documents that may contain PII or CIL protected information when no longer in use.
- Only use secure e-mail or official government computers when discussing any PII or CIL protected information.

OPSEC Measures

JFHQ-NY OPSEC Measures:

- Immediately report any lost or stolen CAC cards, passwords, pins, combinations, keys, or documents to your supervisor and the necessary authorities.
- Do not post any PII or CIL protected information on social networking sites, blogs, or other public internet domains.
- Properly secure equipment and documents at home station and during travel to ensure no items are lost or stolen.

Some OPSEC Measures You Should Practice Online

- **Do not** discuss sensitive information
  - E-mails
  - Chat rooms/instant messaging
  - Blogs
- Avoid posting excessive personal information online
  - Rank/MOS
  - Your family members full names
  - Your address
- **Practice good computer security**
  - **Strong passwords**
  - **Updated antivirus**
  - **Permission/account settings**

Some OPSEC Measures You Should Practice Online

- **Do not** use the same passwords for multiple online sites
- **Do not** depend on the security of the site you're using

- **Do** understand the risks of geotagging

- Blog with caution!!

Questions?

JFHQ OPSEC Manager
SSG David Vetter

518.786.4927

david.a.vetter2.mil@mail.mil