SNS SAFETY CHECKLIST

PERSONAL INFORMATION – DO YOU:

- » Keep sensitive, work-related information OFF your profile?
- » Keep your plans, schedules, and location data to yourself?
- » Protect the names and information of coworkers, friends, and family members?
- » Tell friends to be careful when posting photos and information about you and your family?

POSTED DATA – BEFORE POSTING, DID YOU:

- » Check all photos for indicators of work-related information in the background and reflective surfaces?
- » Check file names and file tags for sensitive data (your name, organization, and other details)?

PASSWORDS – ARE THEY:

- » Unique from your other online passwords?
- » Sufficiently hard to guess?
- » Adequately protected (not shared)?

SETTINGS AND PRIVACY – DID YOU:

- » Carefully look for and set all of your privacy and security options?
- » Determine both your profile and search visibility?
- » Sort “friends” into groups and networks and set access permissions accordingly?
- » Verify through other channels that a “friend” request was actually from your friend?
- » Give new, “untrusted” people with the lowest permissions and accesses to your groups?

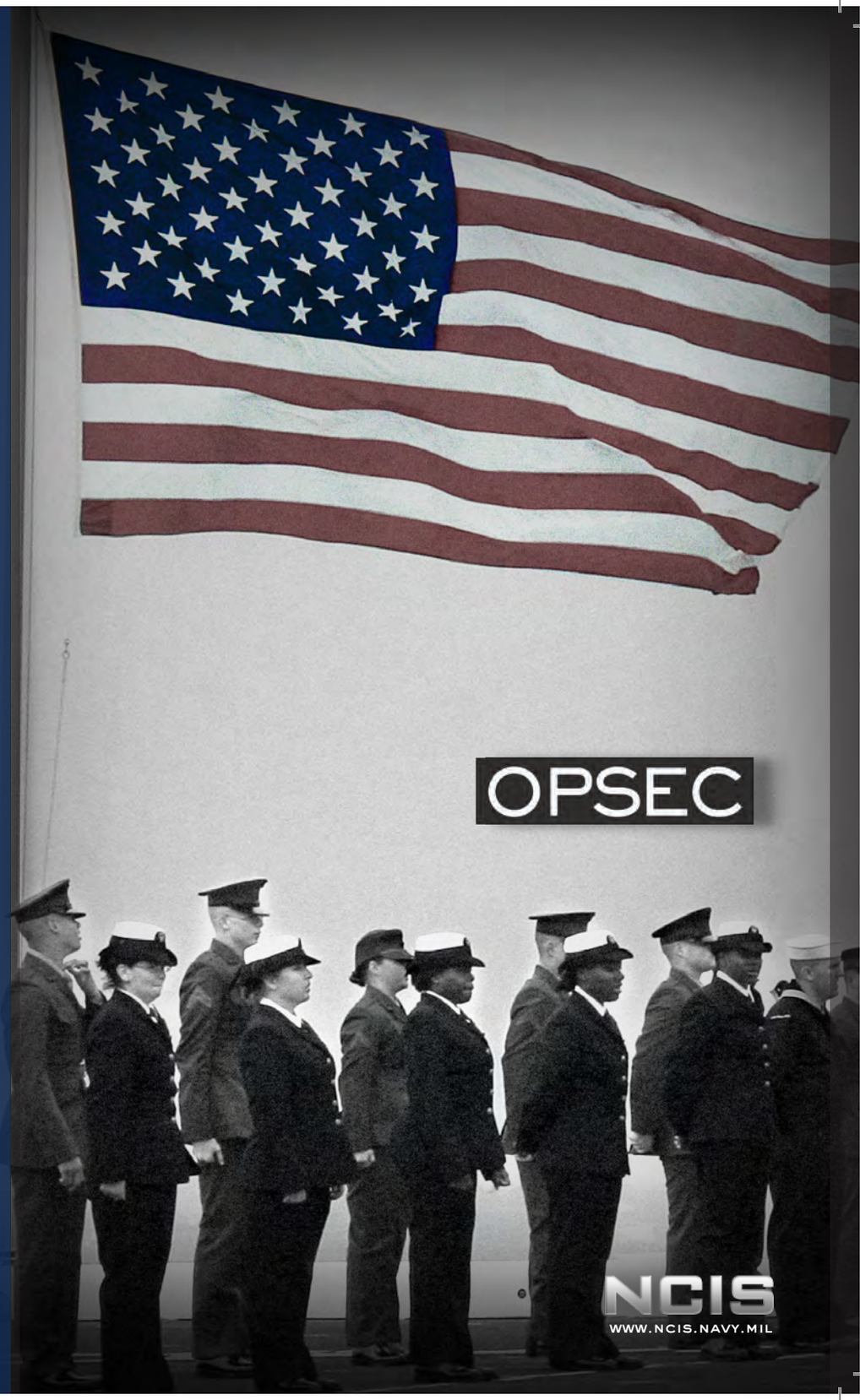
SECURITY – REMEMBER TO:

- » Use and keep security software (anti-virus, anti-spyware, anti-phishing, and firewalls) updated.
- » Beware of links, downloads, and attachments just as you would in emails.
- » Beware of “apps” and plug-ins, which are often written by unknown third parties and could be used to access your data (and your freinds’ data).
- » Look for HTTPS and the lock icon that indicate active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

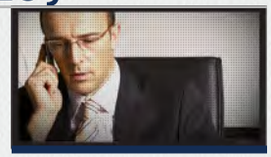
REMEMBER

- » Unclassified information is important, too – pieced together, it can reveal the whole picture.
- » Adversaries do not have to follow legal procedures to collect information.
- » Protecting DON information is everyone’s responsibility.
- » Practicing good OPSEC will help safeguard DON personnel, missions, and facilities.

MAR13



OPERATIONS SECURITY (OPSEC)



OPSEC

Many people believe that if information is not classified, it is OK to share. However, this is not at all accurate. Would you post your full name, birth date, and Social Security number on a bulletin board or website? Would you tape the code to your home's alarm system to your front door? Of course not! Is any of the information classified? No, but you understand the harm that could come from sharing that information with strangers, so you keep it secure. Whether you've realized it or not, you've been practicing OPSEC!

OPSEC focuses on identifying and safeguarding sensitive or critical information, whether it's about you, your family, your coworkers, your overall mission, or your day-to-day operations. Whether we realize it or not, every day there are adversaries, such as terrorists, spies, and criminals, trying to access this type of information. They piece together bits of data, especially open-source information, to determine the big picture related to our missions. Use of OPSEC every day can help make sure this does not happen. Your understanding and use of sound OPSEC practices may save lives… including your own!

THE THREAT

An adversary is any person or group that collects information about the Navy or Marine Corps and intends to use that information to cause harm to operations and assets and includes foreign intelligence organizations, terrorist groups, lone criminals, and organized criminal enterprises.

Adversaries may use multiple methods to collect information:

- Searching trash containers
- Monitoring radio frequencies, cellphones, wireless devices, email, faxes, and telephones
- Monitoring and exploiting the Internet and social media
- Elicitation, eavesdropping, and electronic surveillance

"USING PUBLIC RESOURCES OPENLY & WITHOUT RESORTING TO ILLEGAL MEANS, IT IS POSSIBLE TO GATHER AT LEAST **80%** OF INFORMATION NEEDED ABOUT THE ENEMY."

Source // Al Qaeda Handbook

CRITICAL INFORMATION

Critical information is specific facts about our intentions, capabilities, and activities needed by our adversaries to cause unacceptable consequences for our mission accomplishment. In addition, critical information is any information that you or your mission manager considers sensitive. Here are some examples:

- Names and photos of you, your family, or coworkers
- User names, passwords, and computer and networking information
- Personnel information, including rosters, clearance levels and personal addresses and phone numbers
- Operational, security, and budget information, logistical data
- Mission capabilities or limitations
- Building plans, schedules, and travel itineraries
- Social Security numbers, credit card numbers, and banking info

COUNTERMEASURES

Countermeasures are steps taken to mitigate risk and reduce the loss of critical information. Some countermeasures you should employ include:

- Properly shredding classified and sensitive information, including personally identifiable information
- Using appropriately encrypted radios, telephones, faxes, and email communications
- Never speaking about classified or sensitive information in public
- Always applying the need-to-know principle
- Thinking before you speak
- Adhering to all security and information assurance policies and procedures

OPSEC AND SOCIAL NETWORKING SITES (SNS)

Social networking sites, such as Facebook and Twitter, are great ways to connect with people, share information, and market products and services. However, these sites can also provide adversaries with the critical information they need to disrupt your mission and harm you, your coworkers, or even your family members. Think before you post! Remember, your information could become public at any time due to hacking, configuration changes, social engineering, or the business practice of selling or sharing user data.