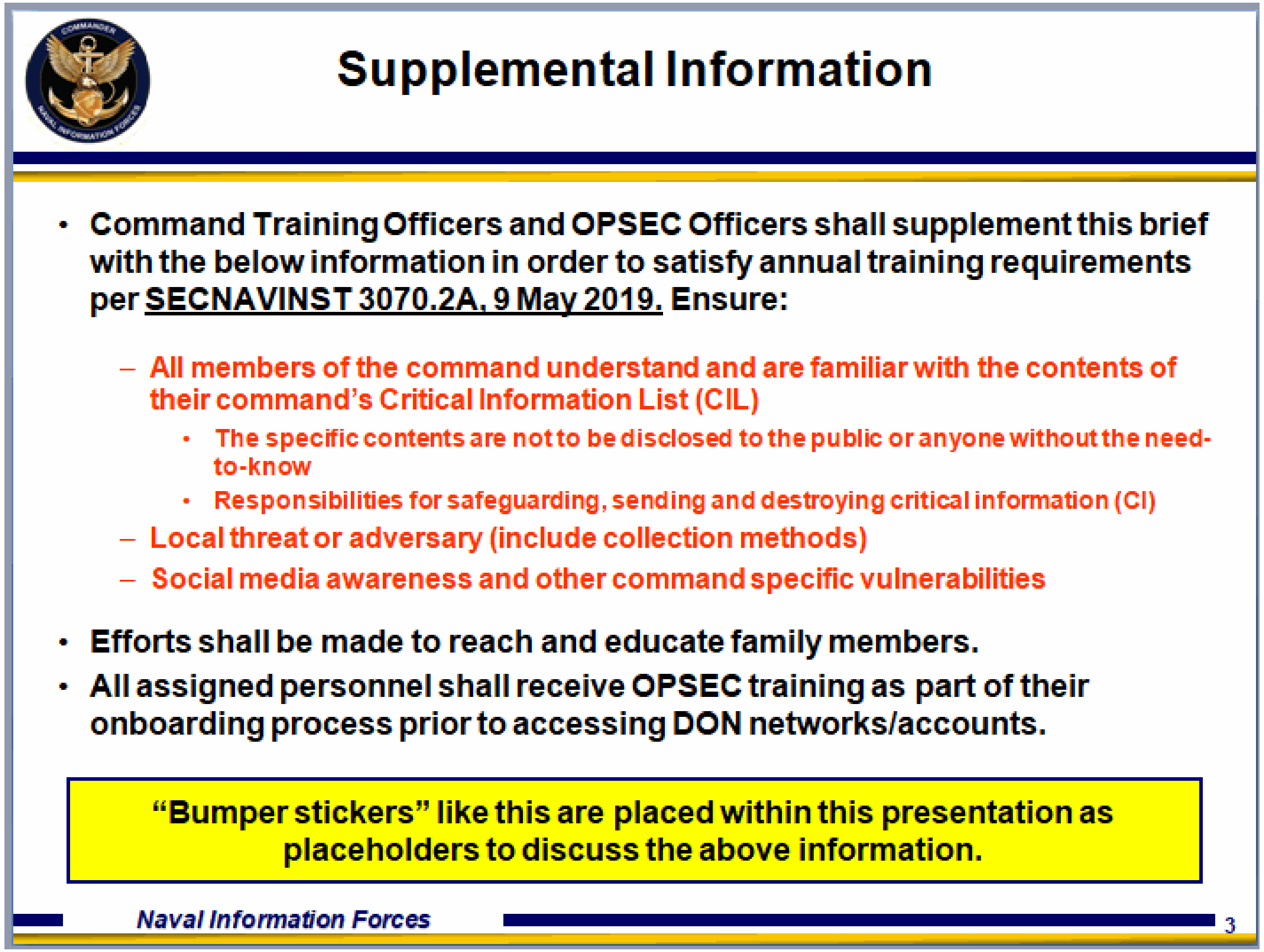
OPSEC
General Military / Annual Training
2022 - 2023

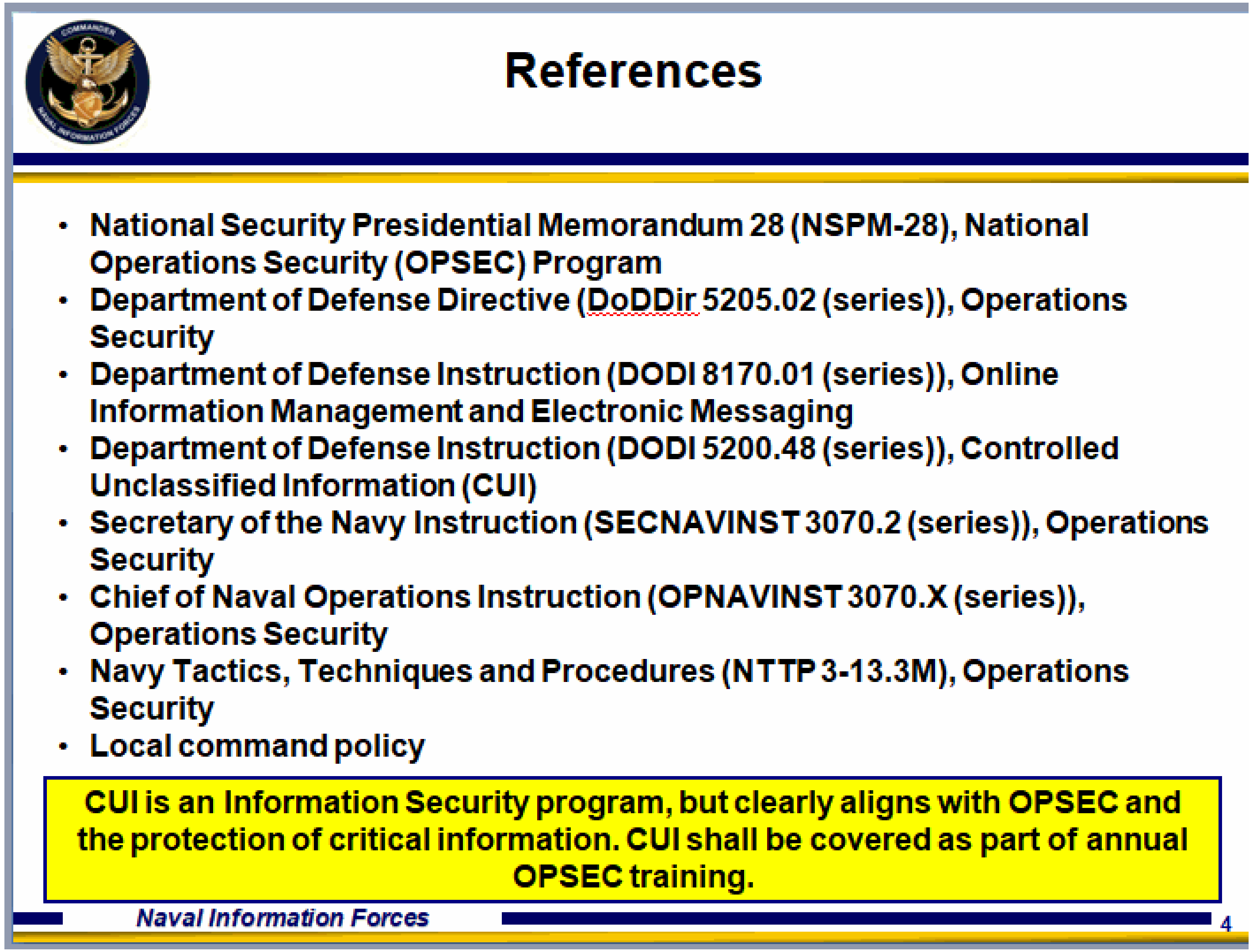
Operations Security (OPSEC)
General Military / Annual Training
2022 - 2023



Supplemental Information

- Command Training Officers and OPSEC Officers shall supplement this brief with the below information in order to satisfy annual training requirements per SECNAVINST 3070.2A, 9 May 2019. Ensure:
  - All members of the command understand and are familiar with the contents of their command's Critical Information List (CIL)
    - The specific contents are not to be disclosed to the public or anyone without the need-to-know
    - Responsibilities for safeguarding, sending and destroying critical information (CI)
  - Local threat or adversary (include collection methods)
  - Social media awareness and other command specific vulnerabilities
- Efforts shall be made to reach and educate family members.
- All assigned personnel shall receive OPSEC training as part of their onboarding process prior to accessing DON networks/accounts.

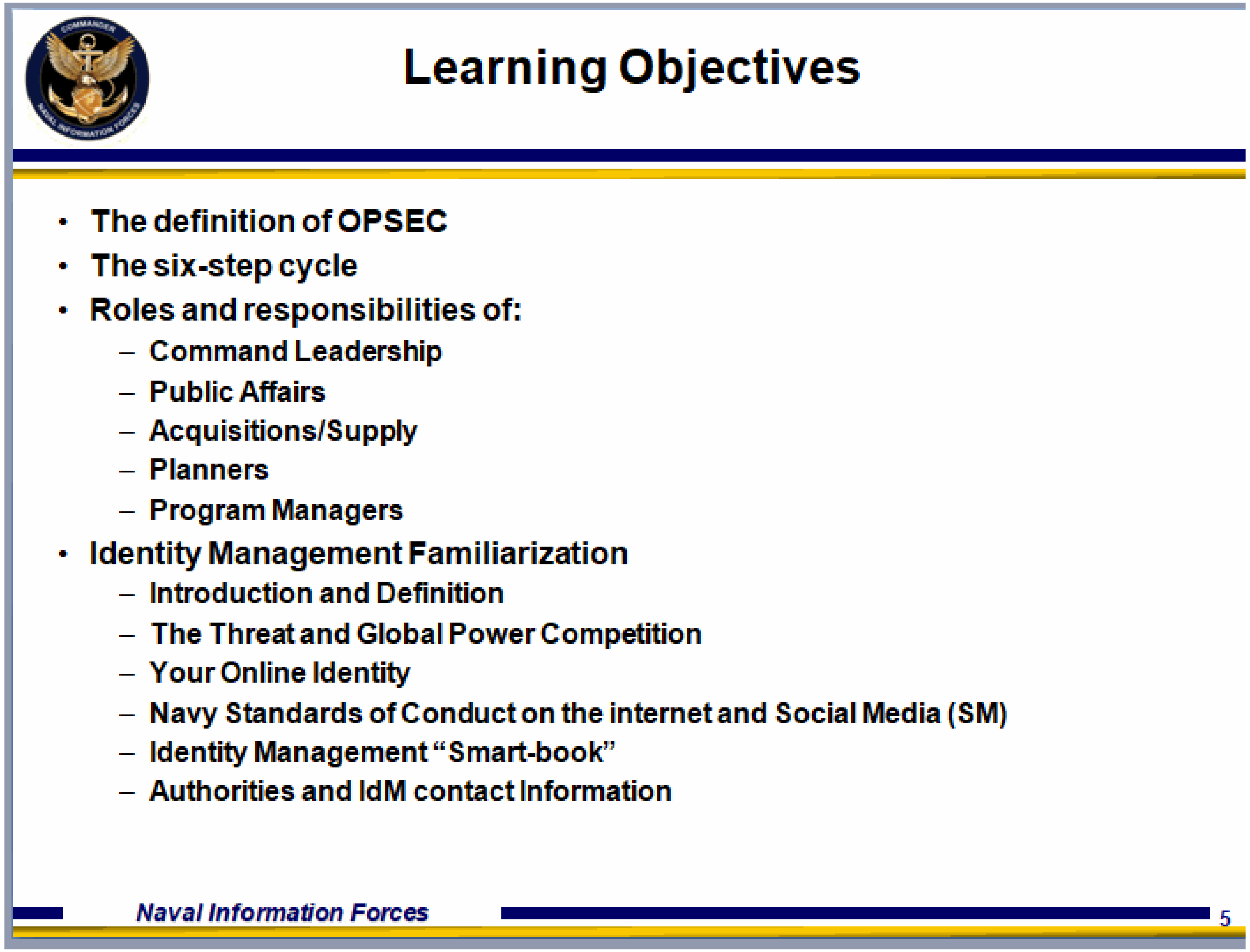
"Bumper stickers" like this are placed within this presentation as placeholders to discuss the above information.



References

- National Security Presidential Memorandum 28 (NSPM-28), National Operations Security (OPSEC) Program
- Department of Defense Directive (DoDDir 5205.02 (series)), Operations Security
- Department of Defense Instruction (DODI 8170.01 (series)), Online Information Management and Electronic Messaging
- Department of Defense Instruction (DODI 5200.48 (series)), Controlled Unclassified Information (CUI)
- Secretary of the Navy Instruction (SECNAVINST 3070.2 (series)), Operations Security
- Chief of Naval Operations Instruction (OPNAVINST 3070.X (series)), Operations Security
- Navy Tactics, Techniques and Procedures (NTTP 3-13.3M), Operations Security
- Local command policy

CUI is an Information Security program, but clearly aligns with OPSEC and the protection of critical information. CUI shall be covered as part of annual OPSEC training.

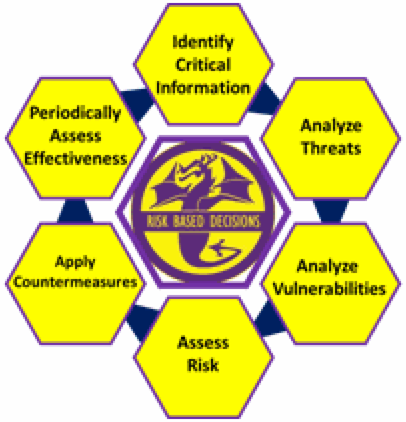


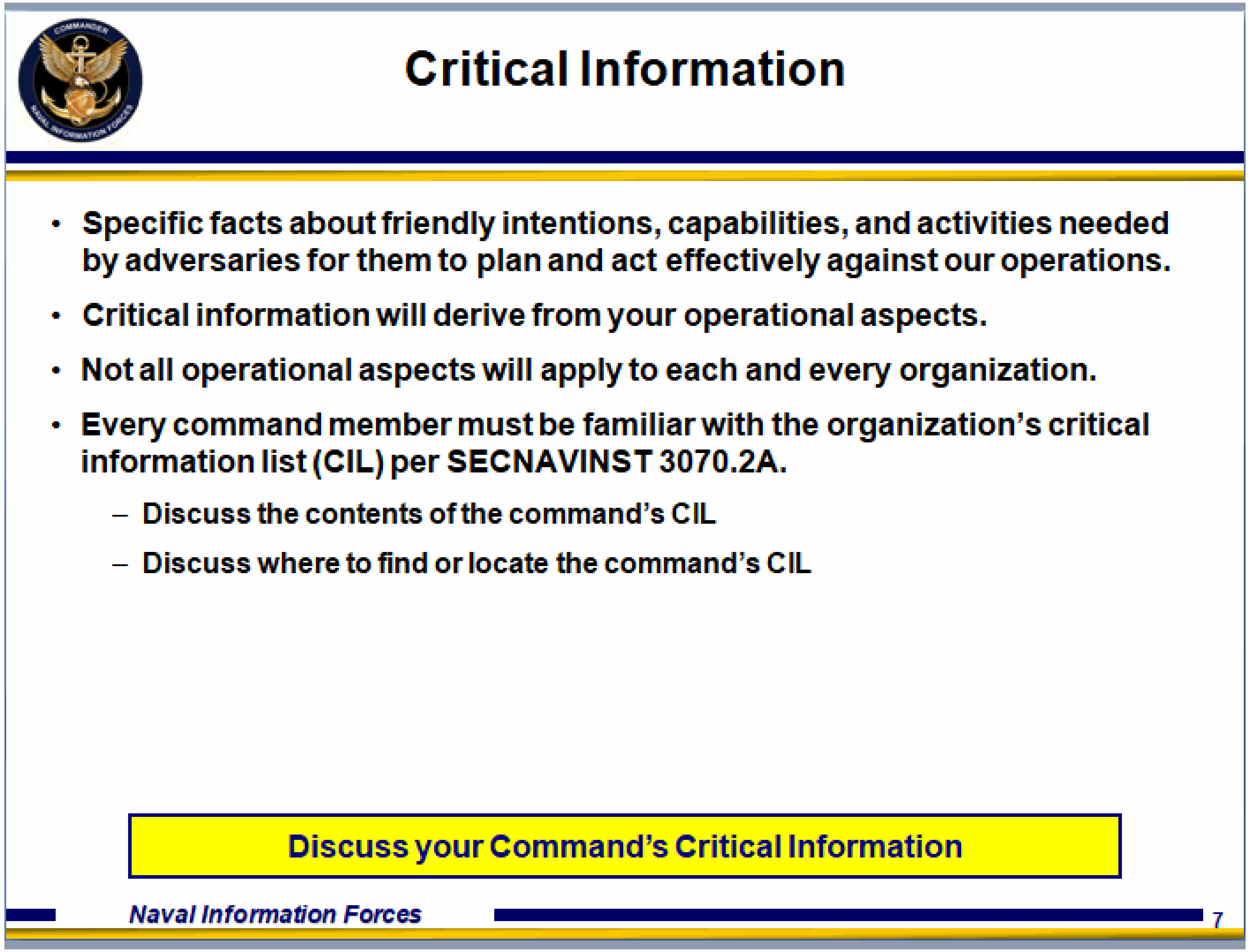
Learning Objectives

- The definition of OPSEC
- The six-step cycle
- Roles and responsibilities of:
  - Command Leadership
  - Public Affairs
  - Acquisitions/Supply
  - Planners
  - Program Managers
- Identity Management Familiarization
  - Introduction and Definition
  - The Threat and Global Power Competition
  - Your Online Identity
  - Navy Standards of Conduct on the internet and Social Media (SM)
  - Identity Management “Smart-book”
  - Authorities and IdM contact Information

Operations Security

- **Operations Security (OPSEC) is a process that identifies unclassified critical information (CI), analyzes potential threats and vulnerabilities, assesses risks, develops countermeasures, and periodically assesses the effectiveness of safeguarding critical information.**
- **OPSEC is one of several Information Related Capabilities (IRC).**
- **Is an operations function that depends on successfully implementing the OPSEC six-step cycle.**
- **The six steps:**
  - **Identify critical information**
  - **Analyze threat**
  - **Analyze vulnerabilities**
  - **Assess risk**
  - **Apply countermeasures**
  - **Periodic assessment of effectiveness**

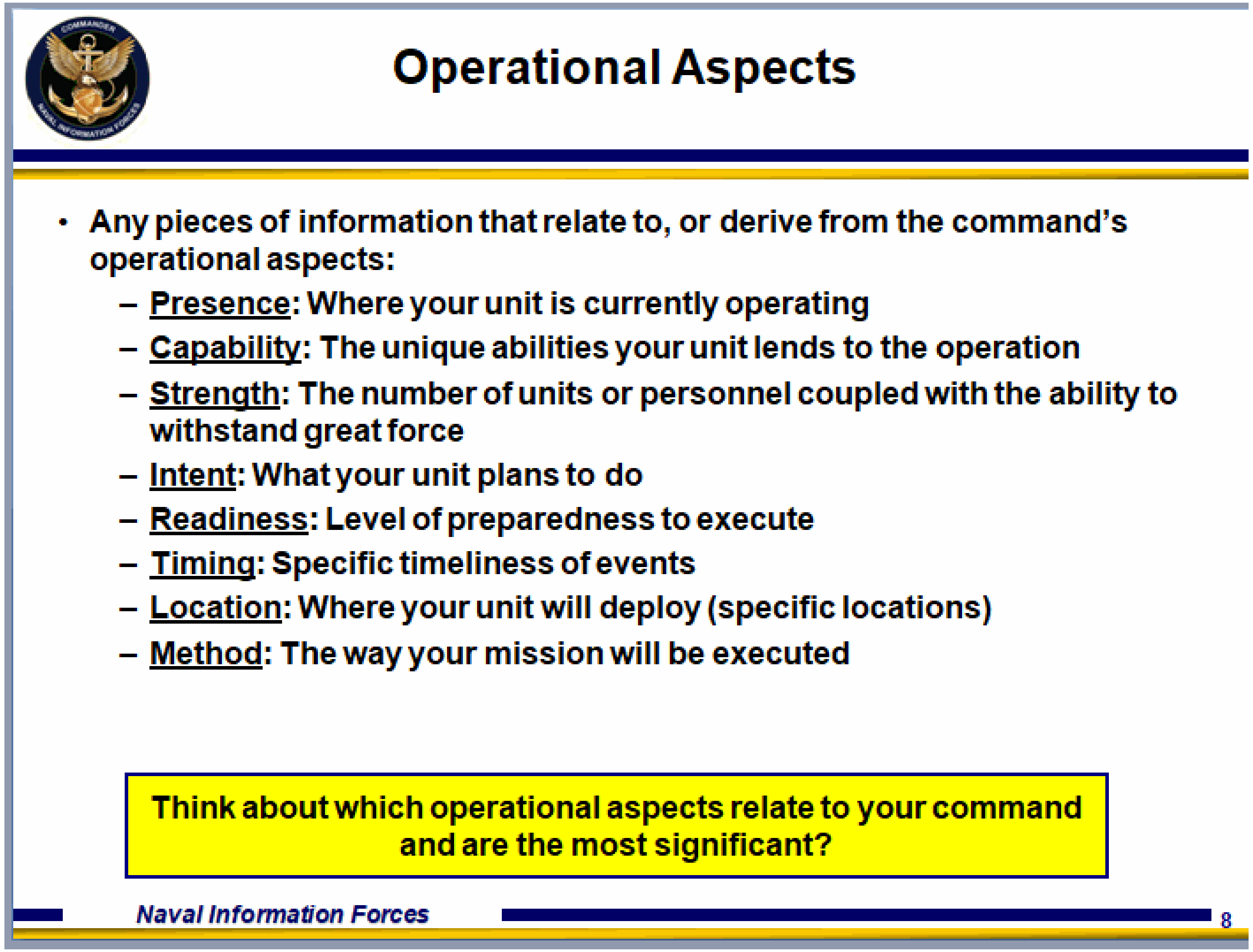




Critical Information

- Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively against our operations.
- Critical information will derive from your operational aspects.
- Not all operational aspects will apply to each and every organization.
- Every command member must be familiar with the organization's critical information list (CIL) per **SECNAVINST 3070.2A.**
  - Discuss the contents of the command's CIL
  - Discuss where to find or locate the command's CIL

Discuss your Command's Critical Information



Operational Aspects

- Any pieces of information that relate to, or derive from the command's operational aspects:
  - Presence: Where your unit is currently operating
  - Capability: The unique abilities your unit lends to the operation
  - Strength: The number of units or personnel coupled with the ability to withstand great force
  - Intent: What your unit plans to do
  - Readiness: Level of preparedness to execute
  - Timing: Specific timeliness of events
  - Location: Where your unit will deploy (specific locations)
  - Method: The way your mission will be executed

Think about which operational aspects relate to your command and are the most significant?

Indicators

- Friendly, detectable actions that potentially reveal critical information:
  - Longer working hours
  - Rehearsals
  - Sudden changes in procedures
  - Troop or stores on-loads
  - Large troop movements
  - Emblems/logos
  - Routine predictable procedures
- Not all indicators can be protected.
- Not all indicators are necessarily bad.

Threat or Adversary

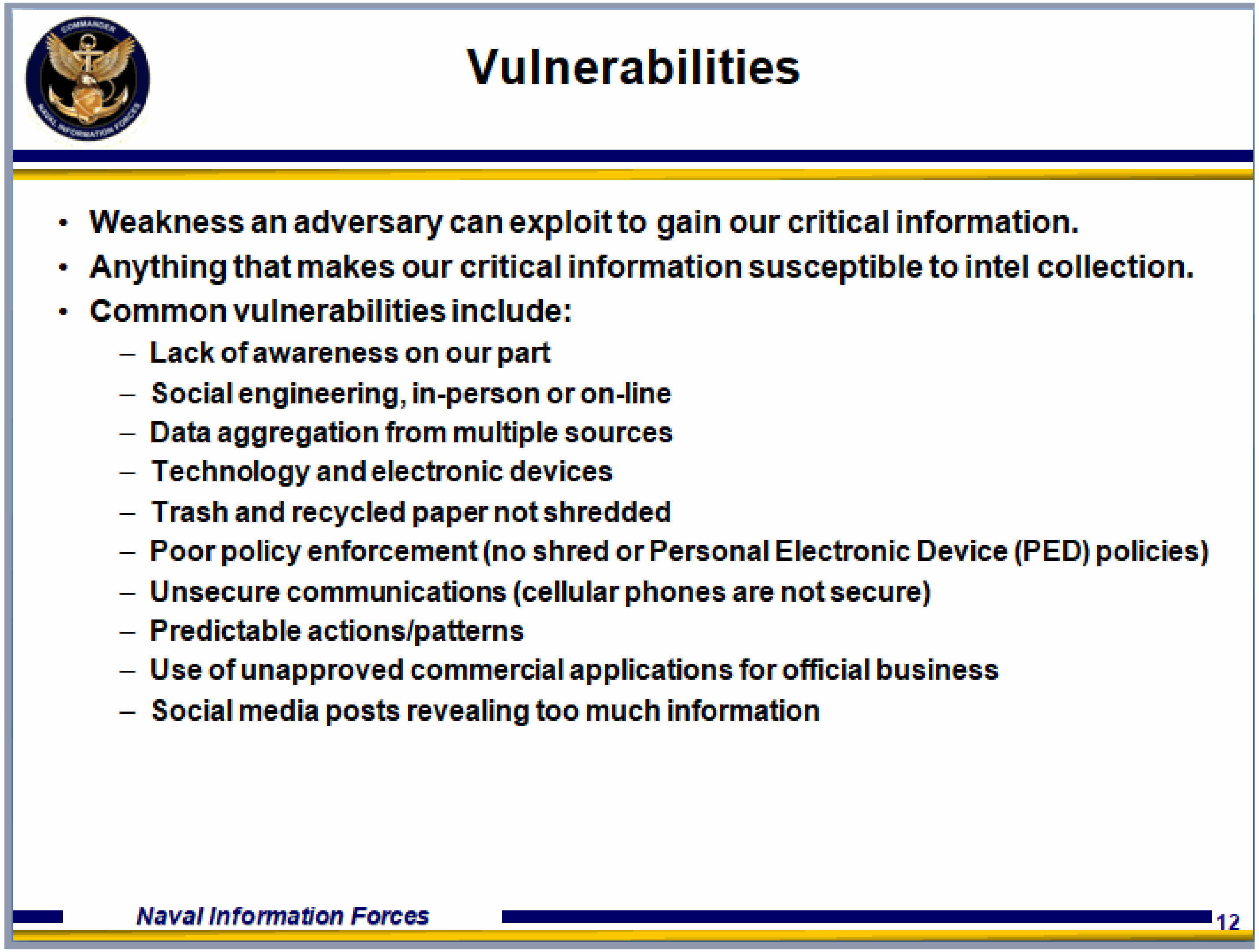
- Capabilities and intentions of an adversary to undertake any action detrimental to the success of friendly activities or operations.
  - Conventional Threats
    - Military opponents
    - Foreign intelligence entities
  - Unconventional Threats
    - Foreign or Domestic Terrorists
    - Insiders (Spies)
- Common Collection Methods:
  - Open Source or Publically Available Information (we provide or post)
  - Human Intelligence (face-to-face and on-line interaction)
  - Signals Intelligence (collection of electronic signals)
  - Geospatial Intelligence (overhead or satellite)
  - Measures and Signatures Intelligence (technically derived signatures)

Discuss your organization's most realistic threat or adversary

What are adversaries looking for?

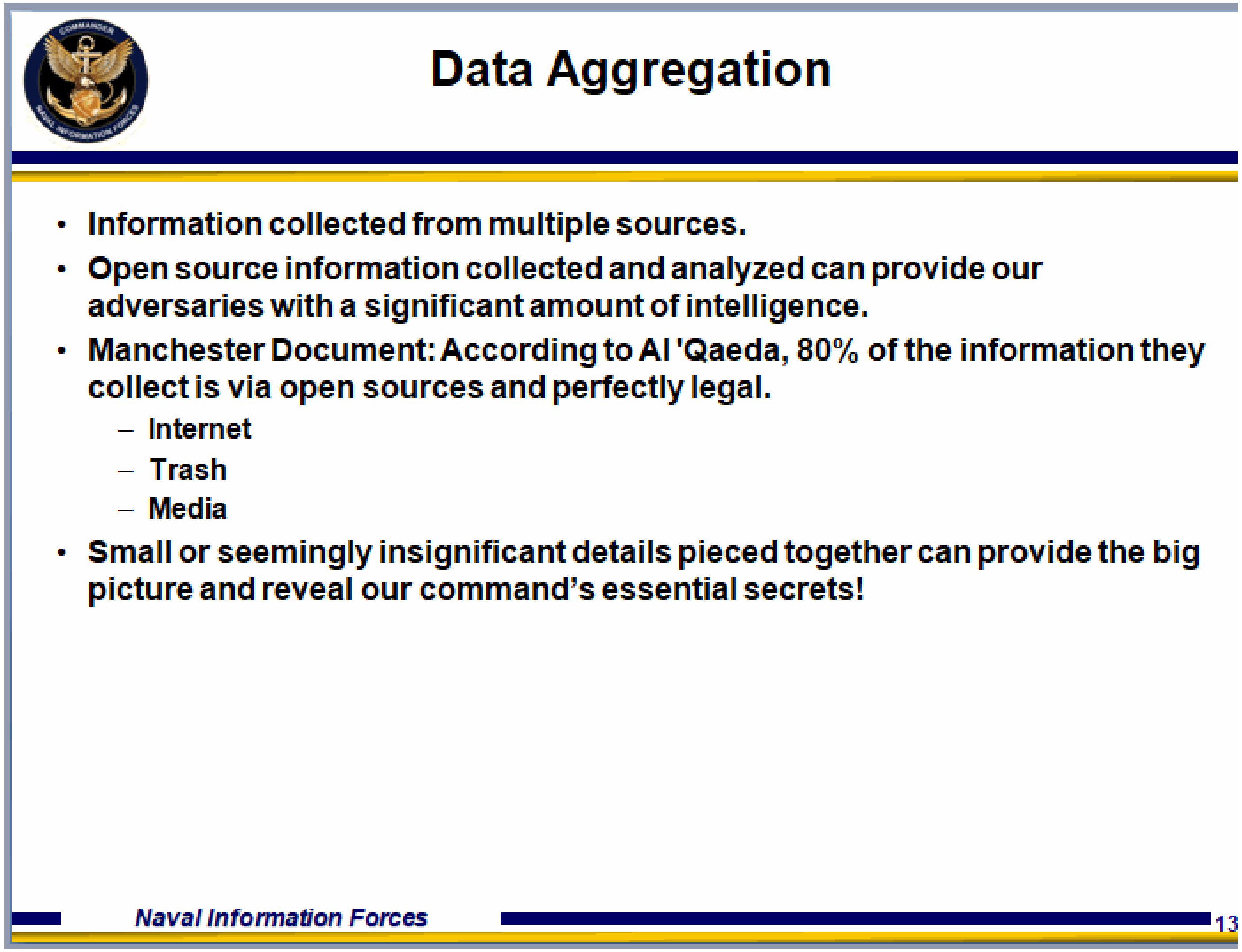
- Operational aspects, critical information and indicators.
- Present, future or sensitive operations:
  - Times of operational events
  - Participating units
  - Projected locations
- Information about military facilities:
  - Location
  - Number of personnel
  - Ammo depot locations
  - Dates and times of operations
- Technology:
  - Develop timelines
  - Determine capabilities and limitations

You may choose to discuss where you can obtain threat data (Organic INTEL, NCIS, etc.)



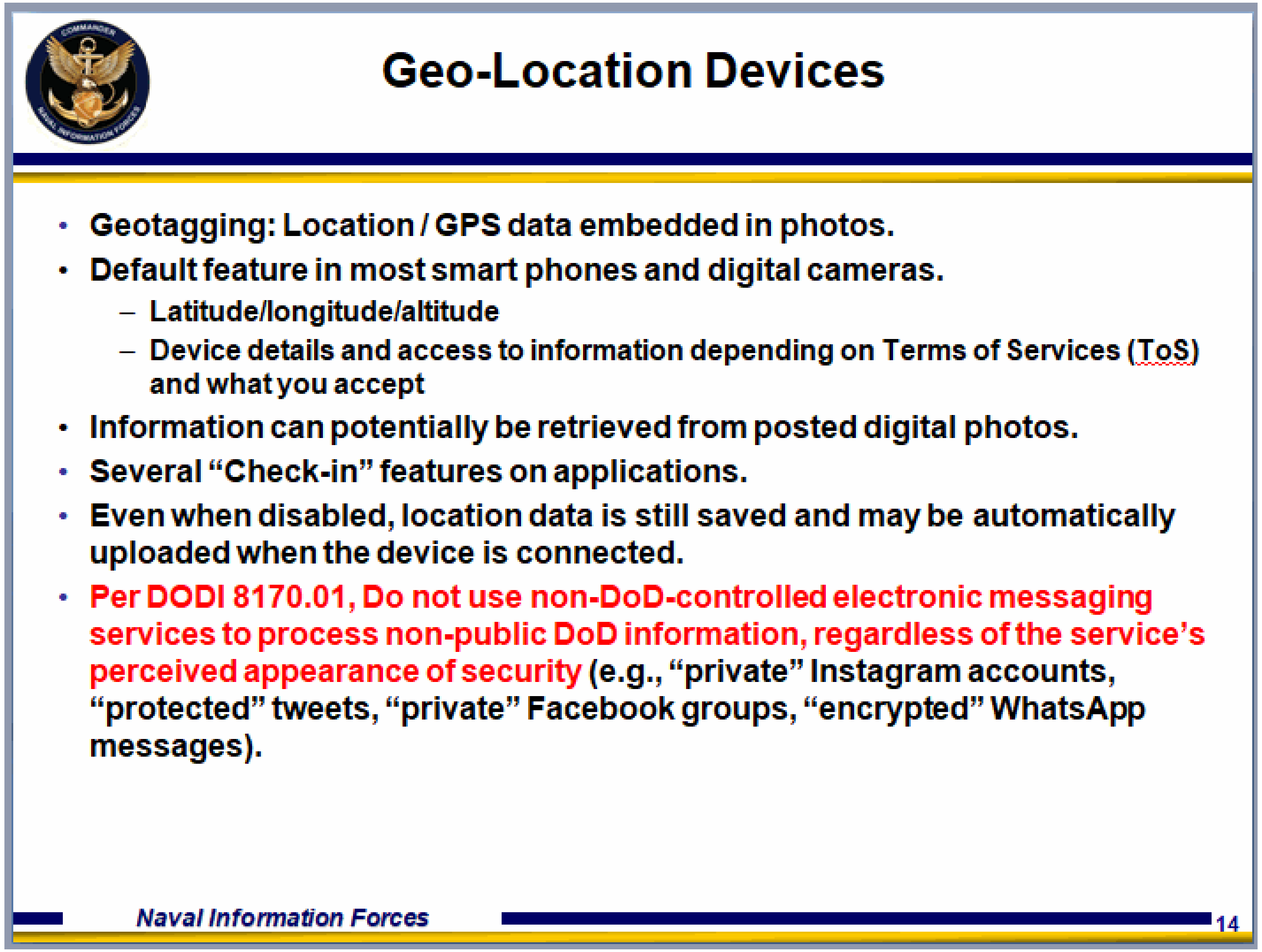
Vulnerabilities

- Weakness an adversary can exploit to gain our critical information.
- Anything that makes our critical information susceptible to intel collection.
- Common vulnerabilities include:
  - Lack of awareness on our part
  - Social engineering, in-person or on-line
  - Data aggregation from multiple sources
  - Technology and electronic devices
  - Trash and recycled paper not shredded
  - Poor policy enforcement (no shred or Personal Electronic Device (PED) policies)
  - Unsecure communications (cellular phones are not secure)
  - Predictable actions/patterns
  - Use of unapproved commercial applications for official business
  - Social media posts revealing too much information



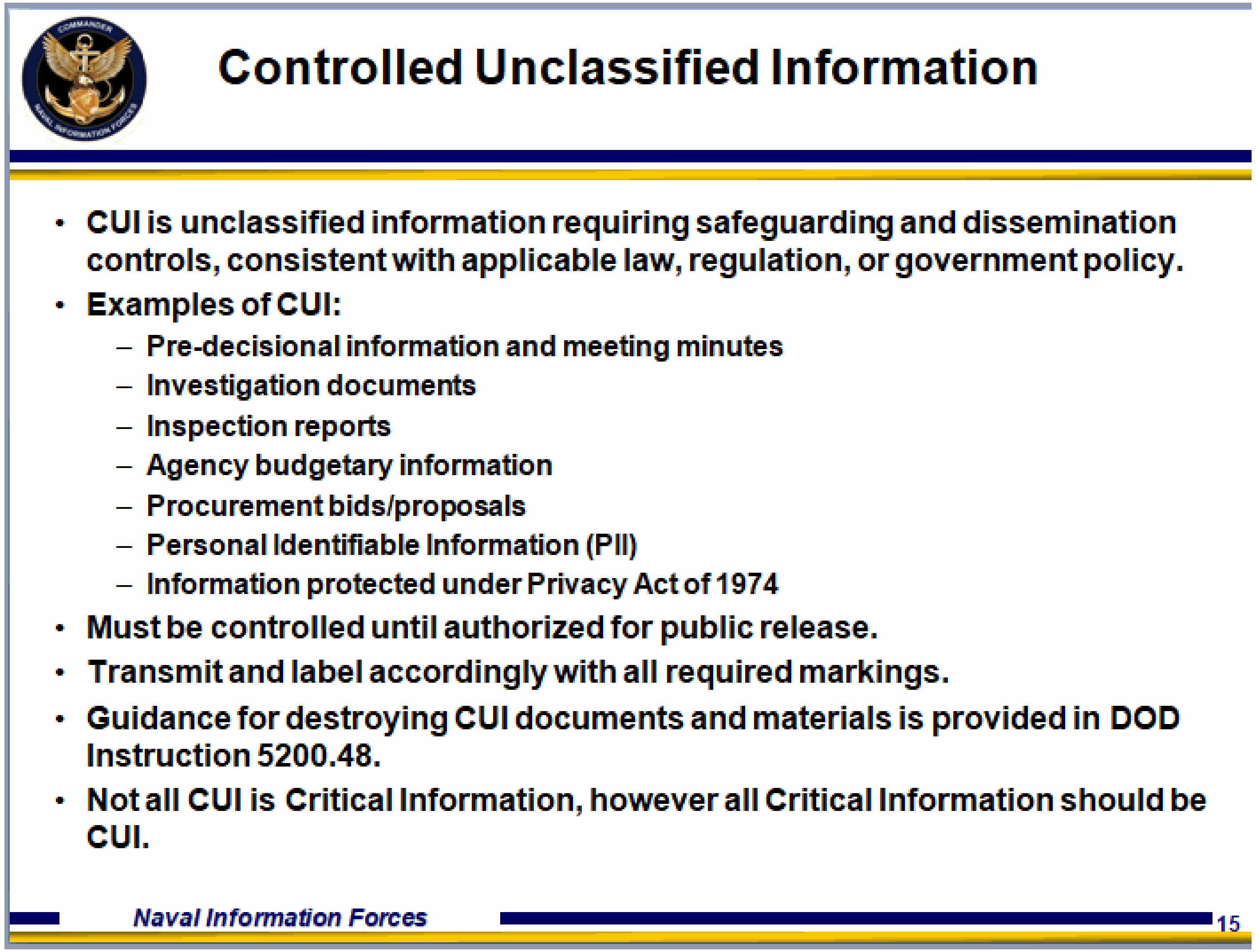
Data Aggregation

- Information collected from multiple sources.
- Open source information collected and analyzed can provide our adversaries with a significant amount of intelligence.
- Manchester Document: According to Al 'Qaeda, 80% of the information they collect is via open sources and perfectly legal.
  - Internet
  - Trash
  - Media
- Small or seemingly insignificant details pieced together can provide the big picture and reveal our command's essential secrets!



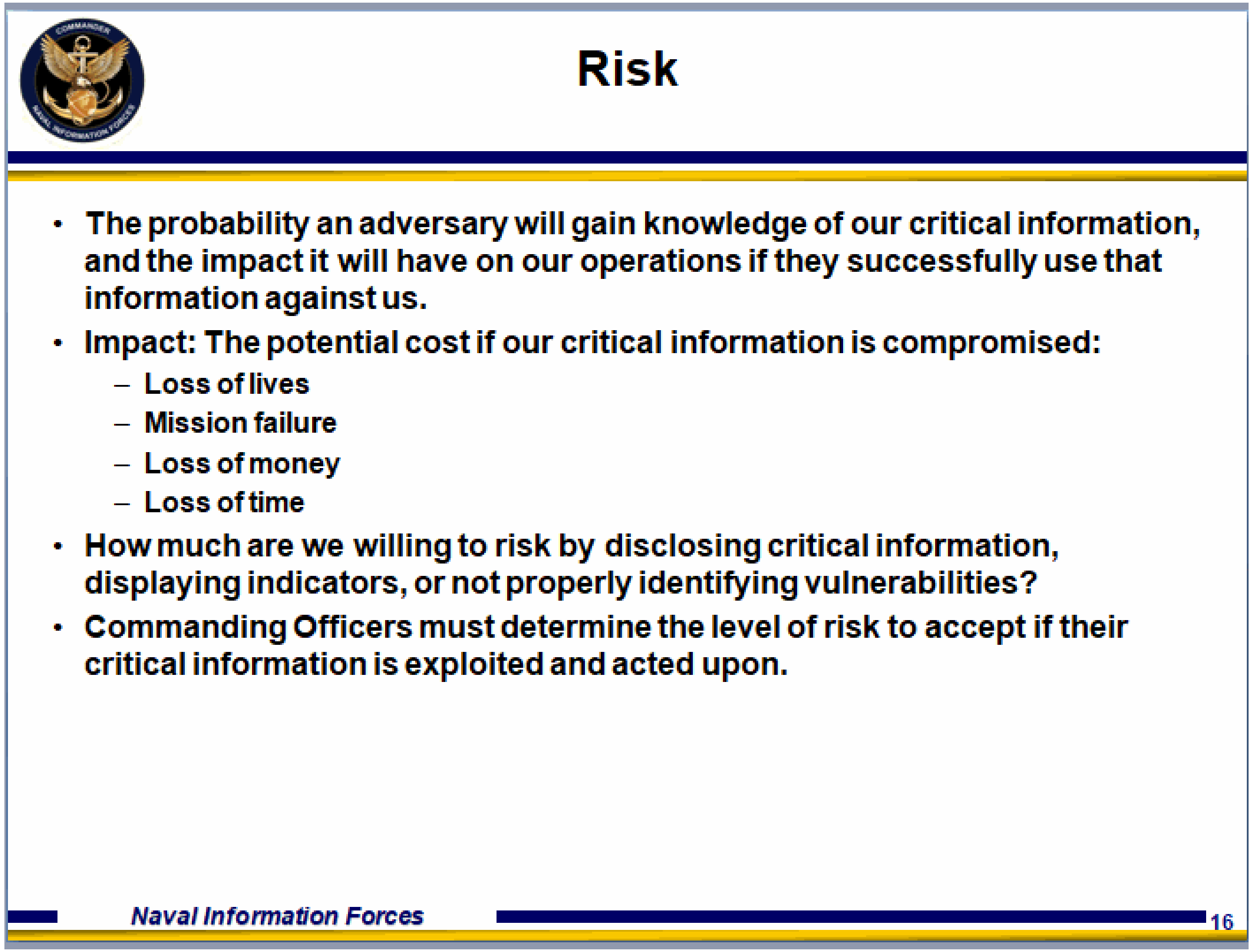
Geo-Location Devices

- Geotagging: Location / GPS data embedded in photos.
- Default feature in most smart phones and digital cameras.
  - Latitude/longitude/altitude
  - Device details and access to information depending on Terms of Services (ToS) and what you accept
- Information can potentially be retrieved from posted digital photos.
- Several "Check-in" features on applications.
- Even when disabled, location data is still saved and may be automatically uploaded when the device is connected.
- Per DODI 8170.01, Do not use non-DoD-controlled electronic messaging services to process non-public DoD information, regardless of the service's perceived appearance of security (e.g., "private" Instagram accounts, "protected" tweets, "private" Facebook groups, "encrypted" WhatsApp messages).



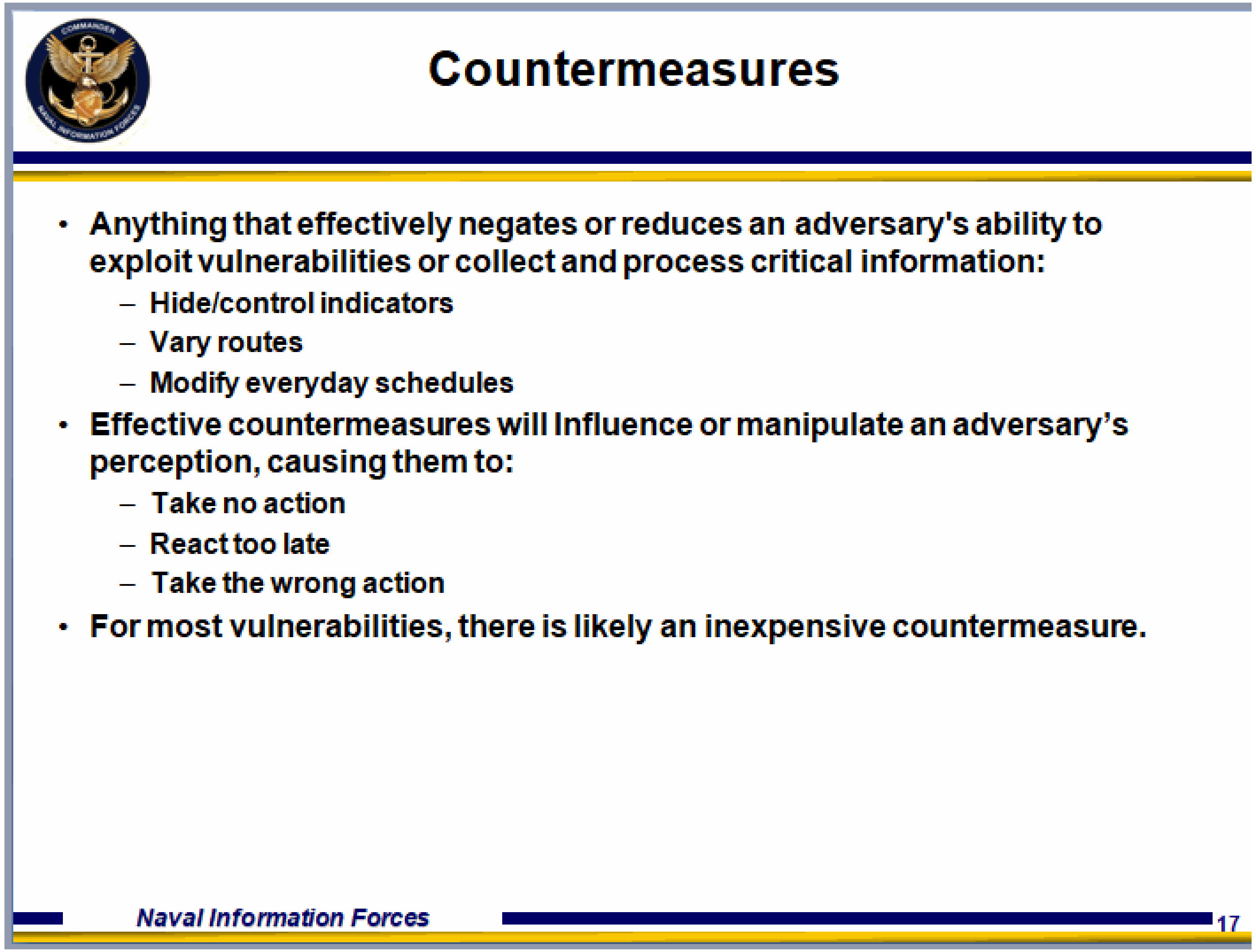
Controlled Unclassified Information

- CUI is unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government policy.
- Examples of CUI:
  - Pre-decisional information and meeting minutes
  - Investigation documents
  - Inspection reports
  - Agency budgetary information
  - Procurement bids/proposals
  - Personal Identifiable Information (PII)
  - Information protected under Privacy Act of 1974
- Must be controlled until authorized for public release.
- Transmit and label accordingly with all required markings.
- Guidance for destroying CUI documents and materials is provided in DOD Instruction 5200.48.
- Not all CUI is Critical Information, however all Critical Information should be CUI.



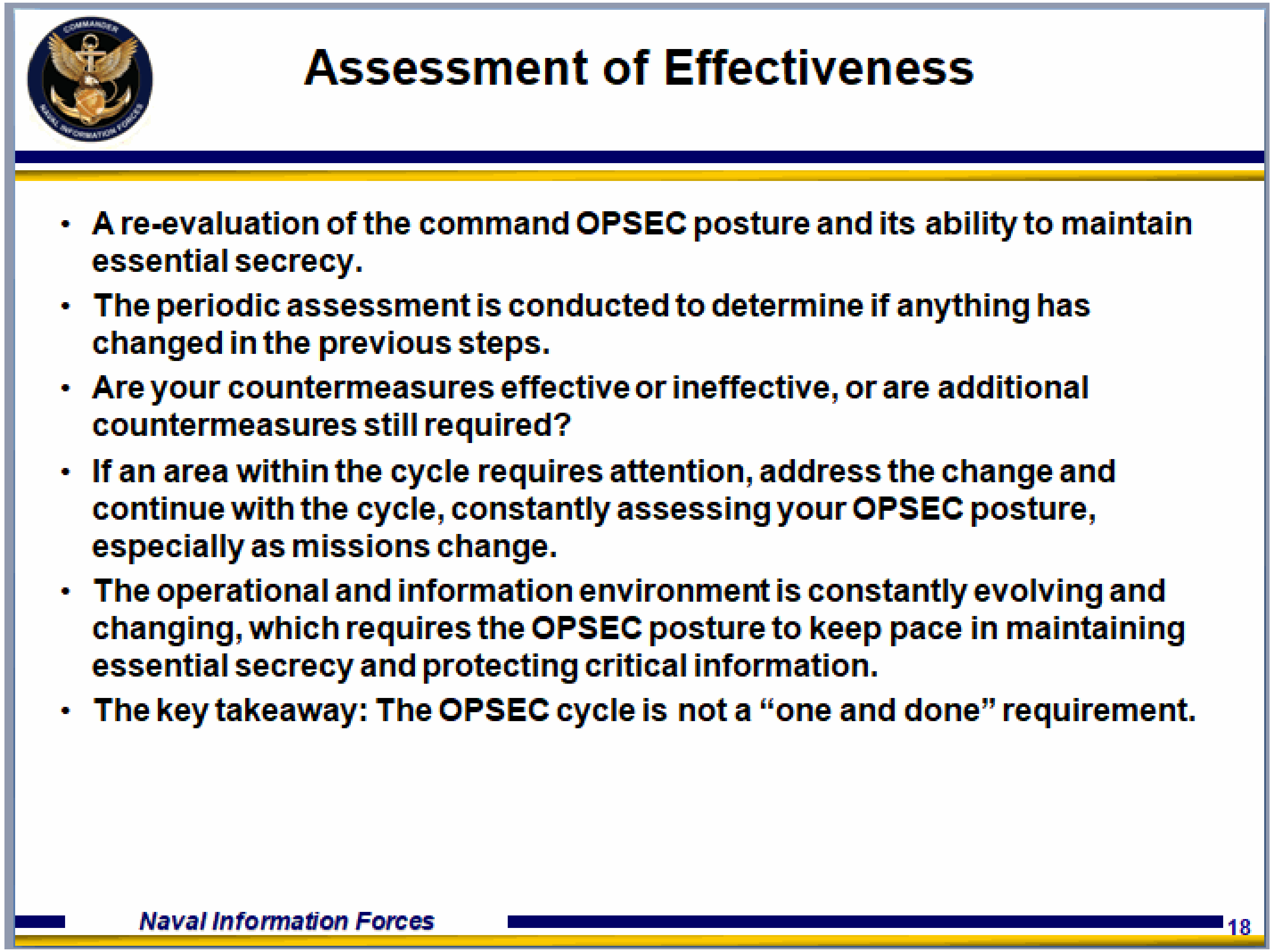
Risk

- The probability an adversary will gain knowledge of our critical information, and the impact it will have on our operations if they successfully use that information against us.
- Impact: The potential cost if our critical information is compromised:
  - Loss of lives
  - Mission failure
  - Loss of money
  - Loss of time
- How much are we willing to risk by disclosing critical information, displaying indicators, or not properly identifying vulnerabilities?
- Commanding Officers must determine the level of risk to accept if their critical information is exploited and acted upon.



Countermeasures

- Anything that effectively negates or reduces an adversary's ability to exploit vulnerabilities or collect and process critical information:
  - Hide/control indicators
  - Vary routes
  - Modify everyday schedules
- Effective countermeasures will Influence or manipulate an adversary’s perception, causing them to:
  - Take no action
  - React too late
  - Take the wrong action
- For most vulnerabilities, there is likely an inexpensive countermeasure.



Assessment of Effectiveness

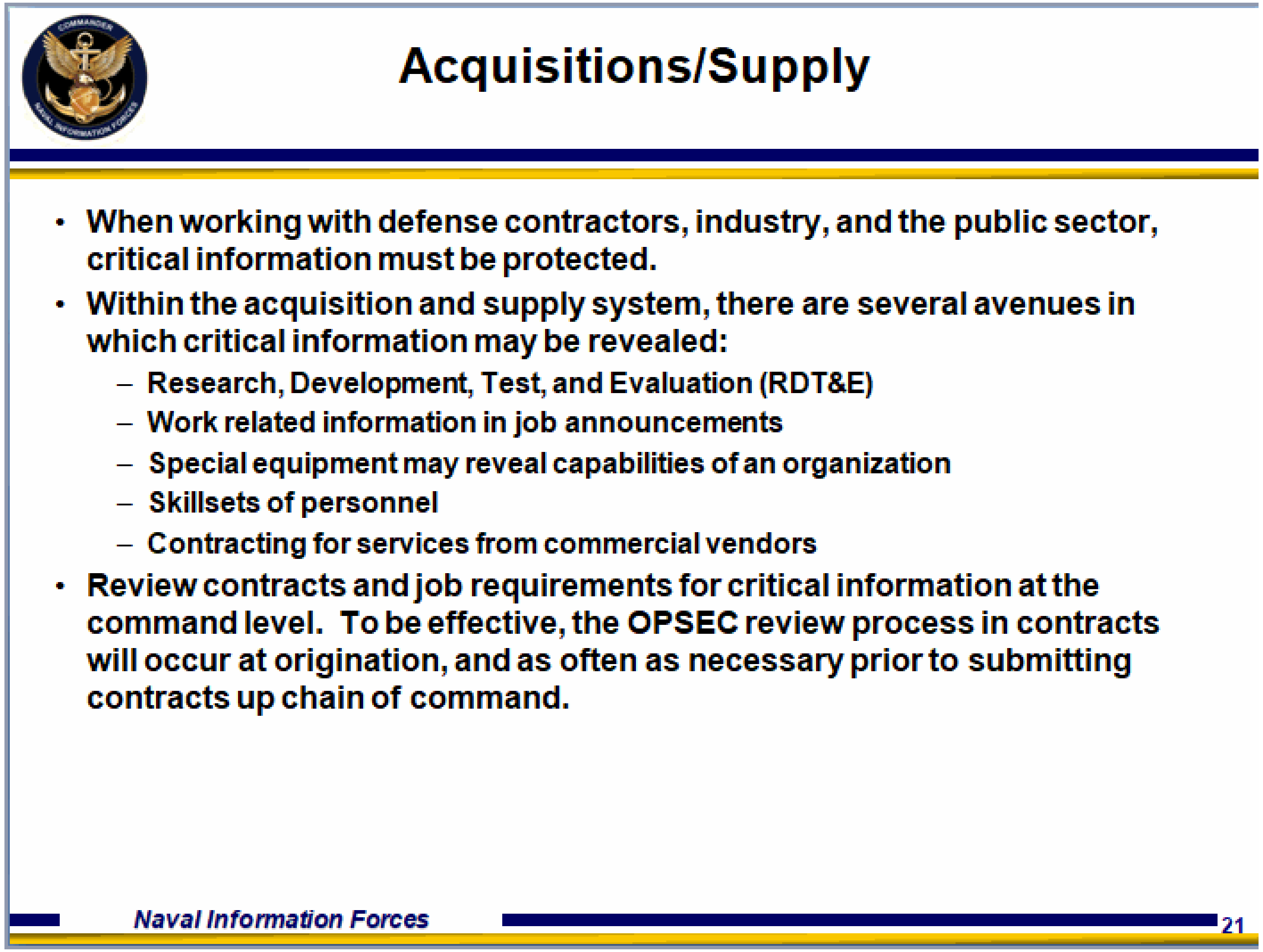
- A re-evaluation of the command OPSEC posture and its ability to maintain essential secrecy.
- The periodic assessment is conducted to determine if anything has changed in the previous steps.
- Are your countermeasures effective or ineffective, or are additional countermeasures still required?
- If an area within the cycle requires attention, address the change and continue with the cycle, constantly assessing your OPSEC posture, especially as missions change.
- The operational and information environment is constantly evolving and changing, which requires the OPSEC posture to keep pace in maintaining essential secrecy and protecting critical information.
- The key takeaway: The OPSEC cycle is not a “one and done” requirement.

Command Leadership

- Own the program and establish policy.
- Establish, resource, and maintain effective OPSEC.
- Provide program managers the resources and authority to execute OPSEC in an effective and efficient manner.
- Take an active role to protect critical information and indicators.
- Ensure effective training and awareness is conducted annually.
- Establish pre-public release review procedures.
- Establish a family outreach program to educate families on the principles of OPSEC and command expectations in sharing and protecting information.
- Develop OPSEC plans when conducting sensitive missions (if applicable).
- Provide oversight and guidance to subordinate elements (if applicable).
- Ensure annual assessments are conducted and vulnerabilities mitigated.
- Identify unacceptable risks and determine which countermeasures to implement.
- Periodically assess OPSEC effectiveness.

Public Affairs

- Collaborate with OPSEC Officers and have a mutual understanding of what information to project and protect; work together.
- Receive specialized OPSEC training.
- Ensure information that is released, only contains the level of detail necessary to convey the message without revealing critical information.
- Have a clear understanding of the command's essential secrets and critical information.
- Participate in the review process prior to releasing command information to the public.
- Use the OPSEC Officer to your advantage as well as command leadership to ensure the information being released is accurate, properly vetted and sends the right message, all without revealing critical information.
- Bottom line is, more information is not necessarily better!

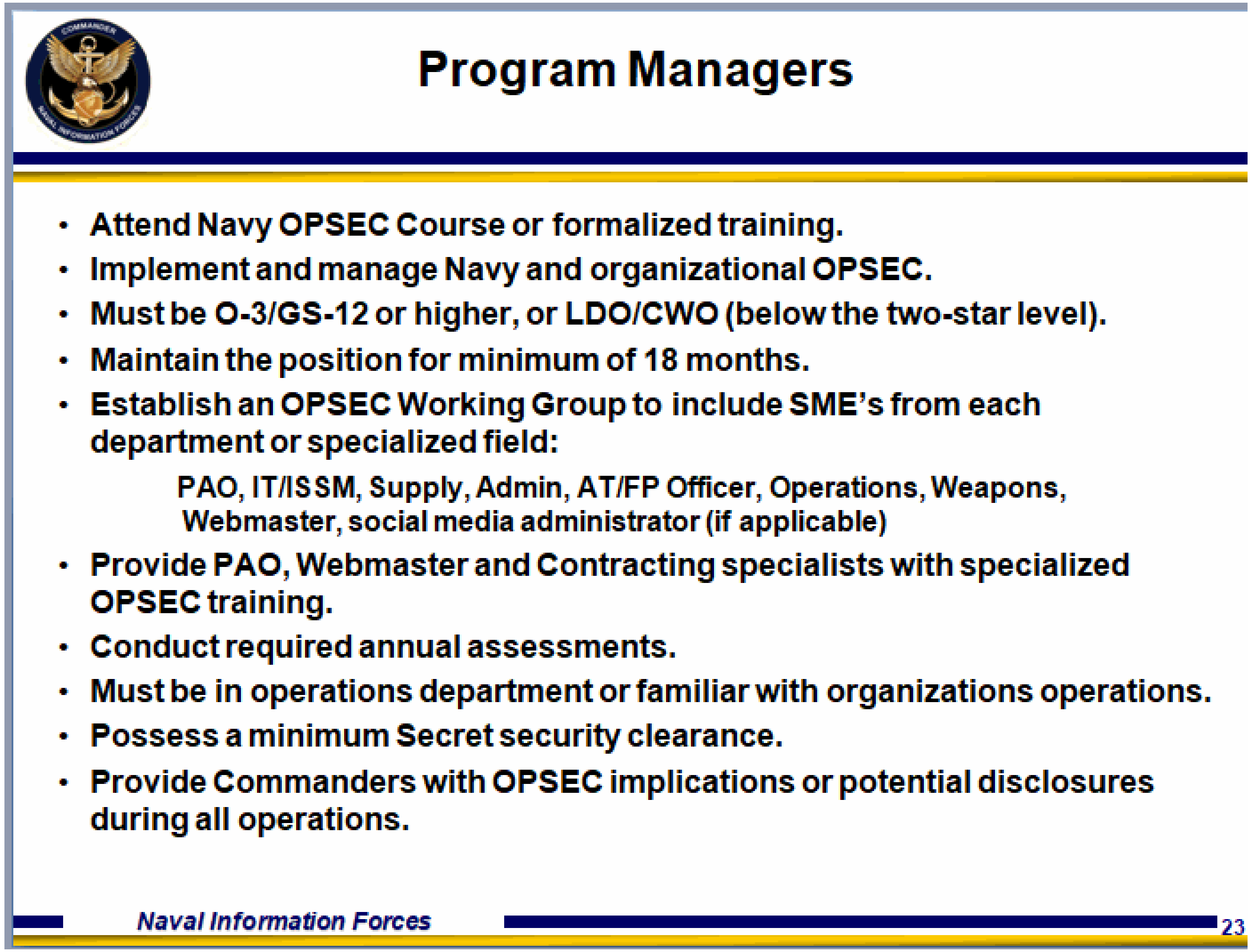


Acquisitions/Supply

- When working with defense contractors, industry, and the public sector, critical information must be protected.
- Within the acquisition and supply system, there are several avenues in which critical information may be revealed:
  - Research, Development, Test, and Evaluation (RDT&E)
  - Work related information in job announcements
  - Special equipment may reveal capabilities of an organization
  - Skillsets of personnel
  - Contracting for services from commercial vendors
- Review contracts and job requirements for critical information at the command level. To be effective, the OPSEC review process in contracts will occur at origination, and as often as necessary prior to submitting contracts up chain of command.

Planners

- Plans should protect observable aspects of friendly operations.
- Most information within these categories should be considered critical:
  - Presence, Capability, Strength, Intent, Readiness, Timing, Location, Methods
    - Adversaries may only need one of these aspects to affect our operations
- OPSEC must be constant.
  - Must maintain essential secrecy and information superiority
- Develop plans in order to manage signatures that reveal critical information, associated indicators, and assigned OPSEC measures for each indicator.
- Ensure OPSEC plans augment (as needed) larger operational plans.
- Include OPSEC in all plans and planning events, from the beginning.
- Maintain OPSEC throughout the entirety of an event or operation.
- Planners should attend the Joint IO Planner course or Defense OPSEC Planner course.

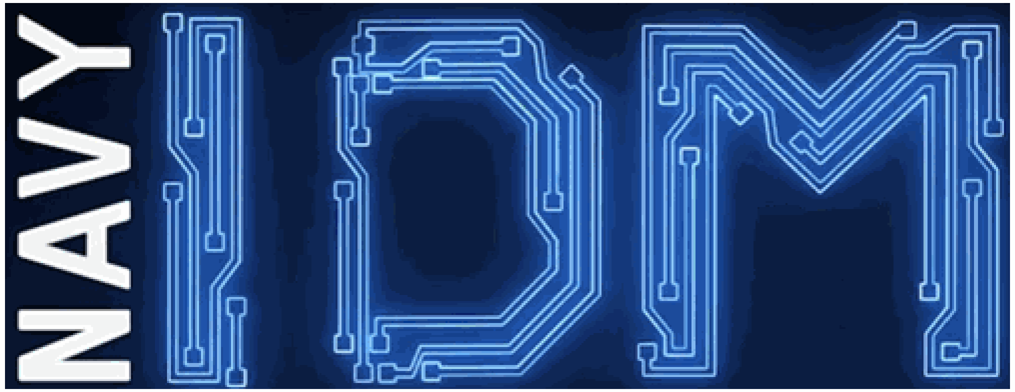


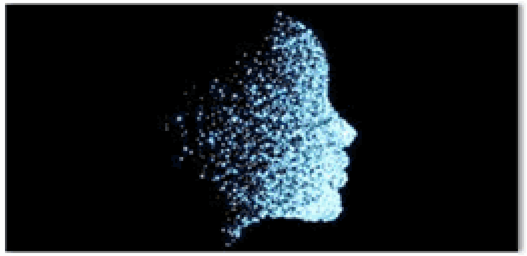
Program Managers

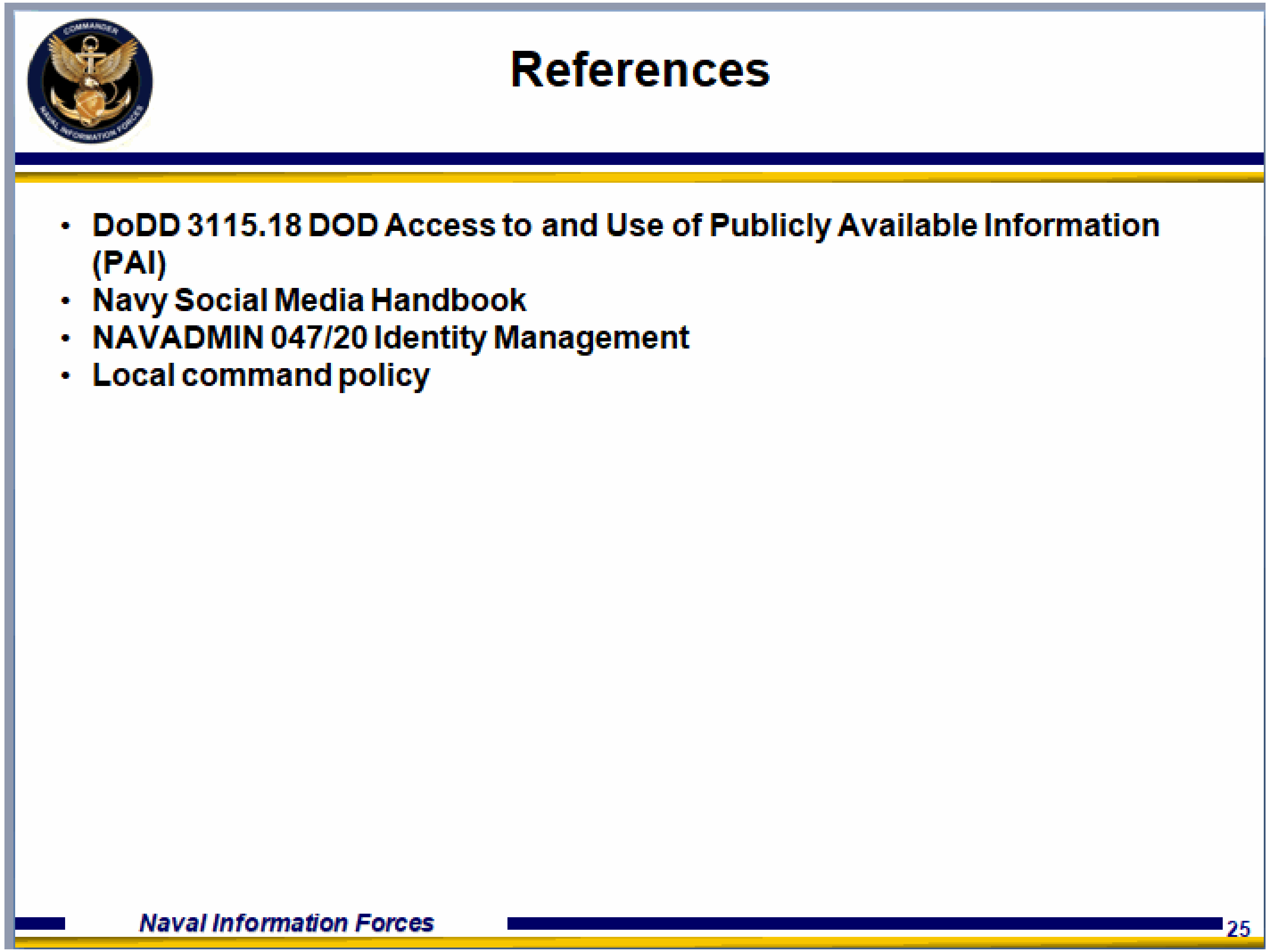
- Attend Navy OPSEC Course or formalized training.
- Implement and manage Navy and organizational OPSEC.
- Must be O-3/GS-12 or higher, or LDO/CWO (below the two-star level).
- Maintain the position for minimum of 18 months.
- Establish an OPSEC Working Group to include SME's from each department or specialized field:

  PAO, IT/ISSM, Supply, Admin, AT/FP Officer, Operations, Weapons, Webmaster, social media administrator (if applicable)
- Provide PAO, Webmaster and Contracting specialists with specialized OPSEC training.
- Conduct required annual assessments.
- Must be in operations department or familiar with organizations operations.
- Possess a minimum Secret security clearance.
- Provide Commanders with OPSEC implications or potential disclosures during all operations.

Identity Management (IdM)





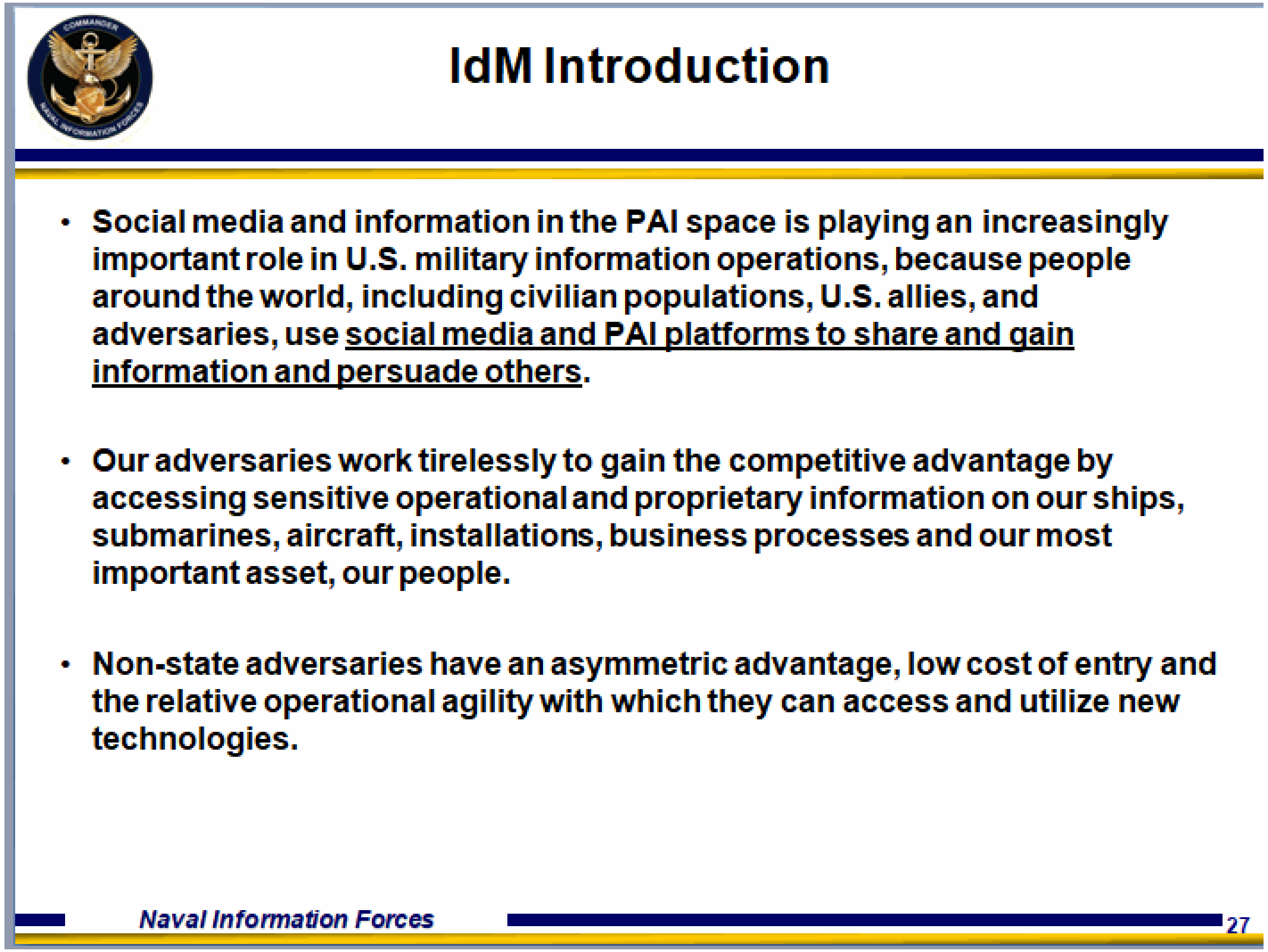


References

- DoDD 3115.18 DOD Access to and Use of Publicly Available Information (PAI)
- Navy Social Media Handbook
- NAVADMIN 047/20 Identity Management
- Local command policy

IdM Definition

- Identity Management (IdM) is a discipline that seeks to mitigate risks to force, mission and capabilities through the discovery, examination, analysis, and assessment of an individual's, or organization's identity elements, characteristics or other attributes in public or non-public records, databases and social media or other unstructured data sources.



IdM Introduction

- Social media and information in the PAI space is playing an increasingly important role in U.S. military information operations, because people around the world, including civilian populations, U.S. allies, and adversaries, use social media and PAI platforms to share and gain information and persuade others.

- Our adversaries work tirelessly to gain the competitive advantage by accessing sensitive operational and proprietary information on our ships, submarines, aircraft, installations, business processes and our most important asset, our people.

- Non-state adversaries have an asymmetric advantage, low cost of entry and the relative operational agility with which they can access and utilize new technologies.

IdM Introduction (cont)

- The Navy is routinely targeted, surveilled and manipulated by adversaries who exploit poor online behavior and practices of our Sailors and families.

- PAI is easily collected, aggregated and analyzed by bad actors to deduce sensitive Navy activities; Presence, Capability, Strength, Intent, Readiness, Timing, Location and Method.

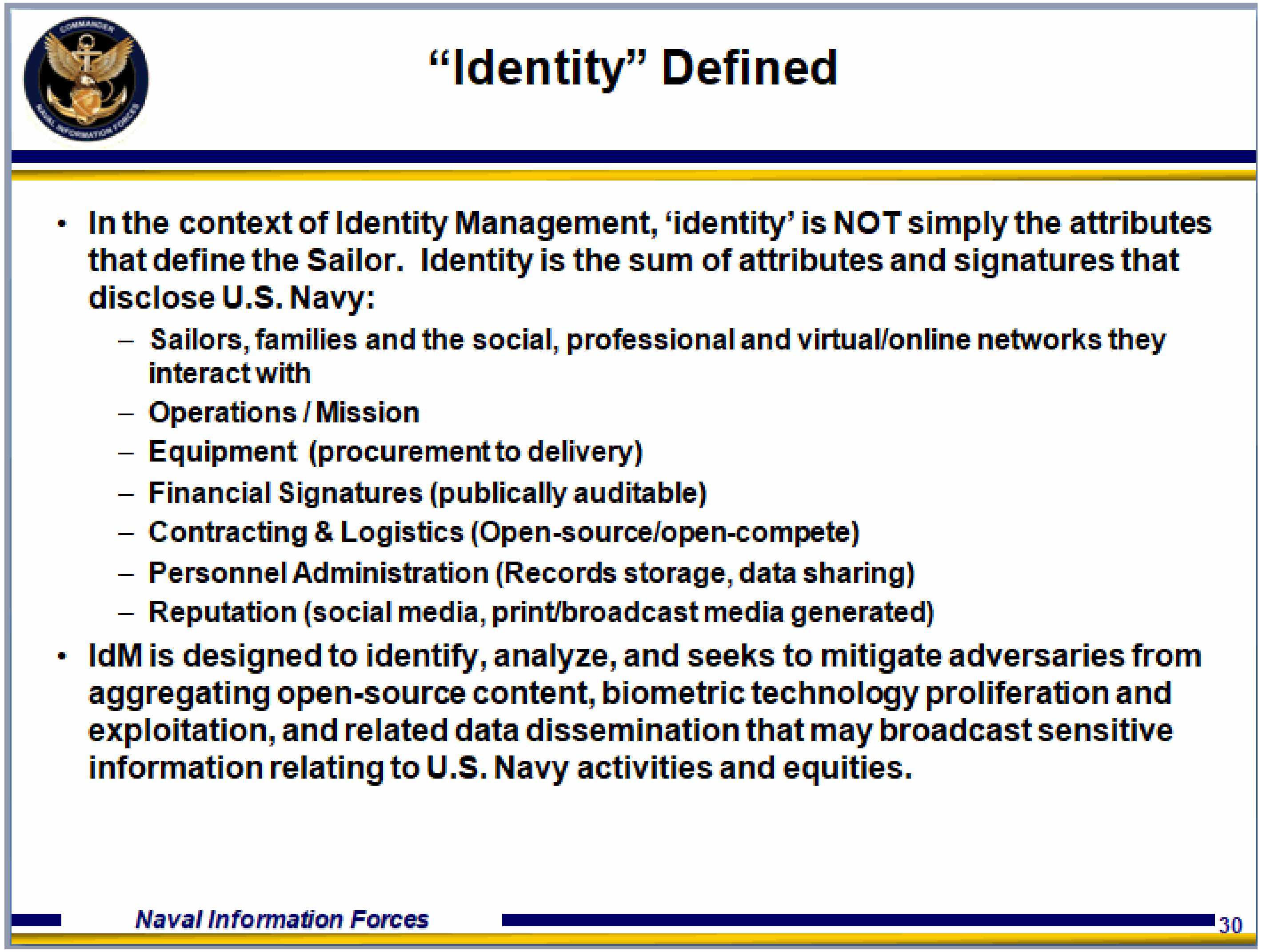
- IdM professionals will monitor the PAI “unmanned battlespace”, in an effort to provide policy, educate, train, mitigate risk and harden a unit’s operational posture.

Threat and Great Power Competition

- Navy platforms, systems, missions, Sailors, and families are routinely monitored, surveilled and manipulated by Great Power Competition (GPC) state and state-sponsored actors via social media, traditional media, open web, and smartphone applications.

- Unwitting Sailors and family members contribute to the problem by providing access to information for GPC actors and cyber-criminals to collect sensitive information and spread misinformation.

- GPC adversaries will continue to exploit PAI in the open-source domain, leaving our platforms, systems, missions, manpower and their families open to intrusion, surveillance, proprietary theft, manipulation and degradation/destruction.



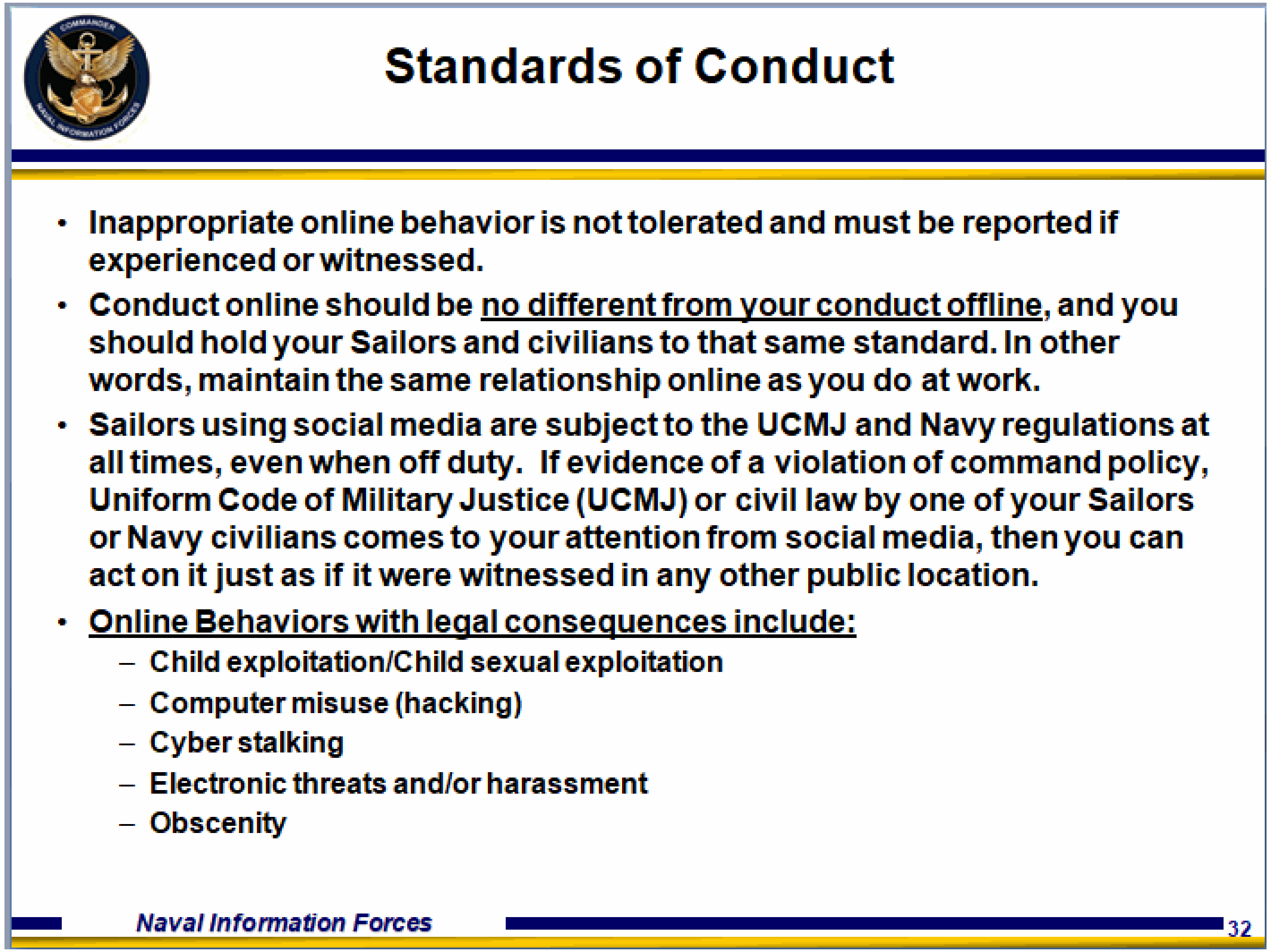
“Identity” Defined

- In the context of Identity Management, ‘identity’ is NOT simply the attributes that define the Sailor. Identity is the sum of attributes and signatures that disclose U.S. Navy:
  - Sailors, families and the social, professional and virtual/online networks they interact with
  - Operations / Mission
  - Equipment (procurement to delivery)
  - Financial Signatures (publically auditable)
  - Contracting & Logistics (Open-source/open-compete)
  - Personnel Administration (Records storage, data sharing)
  - Reputation (social media, print/broadcast media generated)
- IdM is designed to identify, analyze, and seeks to mitigate adversaries from aggregating open-source content, biometric technology proliferation and exploitation, and related data dissemination that may broadcast sensitive information relating to U.S. Navy activities and equities.

Your Digital Identity

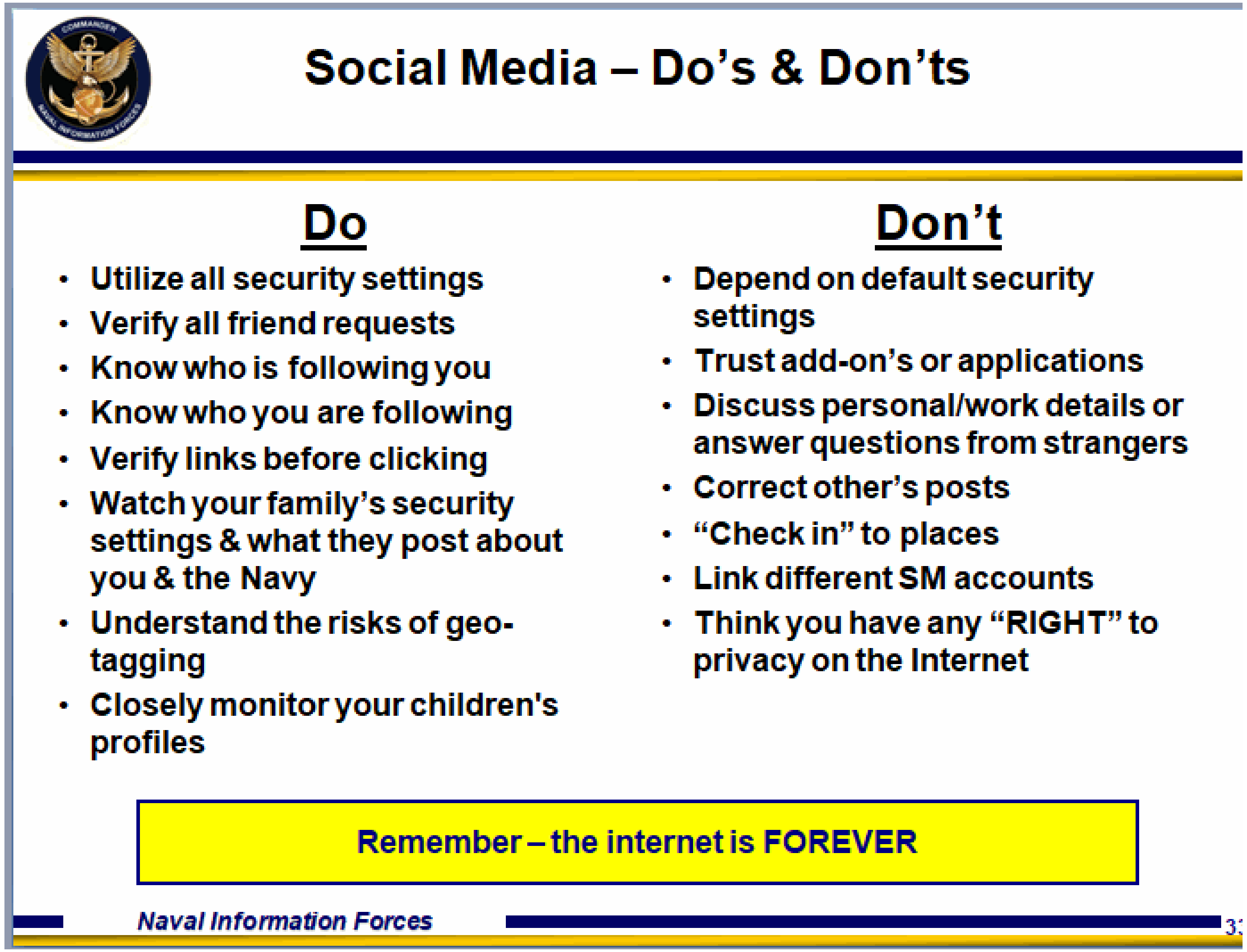
- Military Associated Sites
- Newspapers
- Public Records
  - Legal proceedings and criminal records
  - Birth, adoption, marriage, death, and census records
  - Real estate transactions
  - Voter registration
  - Business licenses
  - Search engines
  - Data aggregators
- Smart Phones and your cellular information
  - Geo-location, texts, photos, etc.
- Frequent Flier, Hotel Rewards, Shopping, etc.
  - Database has extensive records on habits, location, preferences
- Credit Cards
  - Spending habits, location
- Social Networking / Social Media
- Online Gaming

Google yourself – Are you satisfied with your digital footprint



Standards of Conduct

- Inappropriate online behavior is not tolerated and must be reported if experienced or witnessed.
- Conduct online should be no different from your conduct offline, and you should hold your Sailors and civilians to that same standard. In other words, maintain the same relationship online as you do at work.
- Sailors using social media are subject to the UCMJ and Navy regulations at all times, even when off duty. If evidence of a violation of command policy, Uniform Code of Military Justice (UCMJ) or civil law by one of your Sailors or Navy civilians comes to your attention from social media, then you can act on it just as if it were witnessed in any other public location.
- Online Behaviors with legal consequences include:
  - Child exploitation/Child sexual exploitation
  - Computer misuse (hacking)
  - Cyber stalking
  - Electronic threats and/or harassment
  - Obscenity



Social Media – Do's & Don'ts

Do

- Utilize all security settings
- Verify all friend requests
- Know who is following you
- Know who you are following
- Verify links before clicking
- Watch your family's security settings & what they post about you & the Navy
- Understand the risks of geo-tagging
- Closely monitor your children's profiles

Don't

- Depend on default security settings
- Trust add-on's or applications
- Discuss personal/work details or answer questions from strangers
- Correct other's posts
- "Check in" to places
- Link different SM accounts
- Think you have any "RIGHT" to privacy on the Internet

Remember – the internet is FOREVER

PAI – Safety Measures

- Disclosures occur when personnel share information with people they don’t know, or their social media privacy settings are open.

- Personnel who use Social Media shall at a minimum:
  - Ensure all information about any DoD, military and Navy activity and event is approved for public release prior to sharing publicly.
  - Not discuss details of command tactics, techniques or procedures in any social media forum.
  - Not discuss details, capabilities or functions of weapon systems unless specifically authorized.
  - Not provide information of ship/unit locations, itineraries, current or future deployment dates, present or future operational information, unless specifically authorized.
  - Not post any unauthorized pictures, videos, maps, diagrams that identify weapon systems, computer systems, sensitive compartments, radar/sonar, or any other equipment that can compromise capabilities or Tactics, Techniques and Procedures (TTPs).

The Tool to Help

Identity Management Smart-book

- **Gives Sailors and their families very detailed steps to safely set-up/lock-down social media and online digital personal information accounts.**
- **Available for download on Navy CHINFO social and digital media resources.**

Contact Information

For Operations Security, please contact:

Naval Information Forces
115 Lake View Parkway
Suffolk, VA 23435
757-203-3656
opsec@navy.mil
opsec@navy.smil.mil

www.navifor.usff.navy.mil/opsec

Youtube.com/USNOPSEC

For Identity Management, please contact:

Mr. Chris Beam, IdM Deputy Director
christopher.l.beam.civ@us.navy.mil

CDR Barry Shumate, Navy LNO/OPS
(Virginia Beach, VA)
barry.shumate@navy.mil
Office: 757-492-5629

Mr. Robert Lamb, Senior Analyst
robert.j.lamb.civ@us.navy.mil
Mobile: 571-236-7918

Congratulations!
You have completed this training

Please continue to obtain your certificate of completion

Certificate of Achievement

This certificate is award to

Enter Your Name Here

Thursday, December 30, 2021

For completion of the

DON Mandatory
Operations Security Training