

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



Day 2 - New Employee Onboarding

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Human Resources Division
- Staffing Branch

Larry Tarasek
Technical Director, NSWCCD

WELCOME BACK!



Access your onboarding presentation slides on the Carderock New Hires Page :

<https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Carderock/Career-Opportunities/Forms-for-New-Hires>

Once you have obtained your CAC, use the link below to available more useful onboarding materials on your NMCI computer (CAC required):

<https://wiki.navsea.navy.mil/display/WDP/Employee+Onboarding+Program>



Onboarding – Day 2



Agenda

Day 2

- 0800 Roll Call / Day 1 Recap
- 0815 Military Protocol Brief
- 0845 Command Evaluation & Review Brief
- 0900 STEM / New Hire Bridge
- 0920 **Break 1**
- 0930 Initial Security and Indoctrination Brief
- 1000 Controlled Unclassified Information & Privacy & Personally Identifiable Information
- 1030 Uncle Sam's Operations Security Training (OPSEC)
- 1100 Antiterrorism Level I and Active Shooter Training
- 1130 **Lunch**
- 1230 Physical Security Training Insider Threat Training
- 1300 NCIS Training (Counterintelligence Awareness and Reporting Course – CIAR)
- 1330 Safety Briefing
- 1400 Workforce Development Overview
- 1415 Wrap-up / Questions / Survey



Last Updated 12 October 2021



Topics to be Covered



- **Department of Navy (DoN) Civilians**
- **Military Personnel**
- **Addressing Military Personnel**
- **Navy Terminology**
- **Some Basic Navy Customs**
- **Riding a Ship**



Life as a DoN Civilian



Working as a DoN civilian places you in a different culture from a standard position in private industry.

Generally, you will work with and for civilians, but there are some differences between our work environment and private industry you should know...

- Our command chief executive is a Navy Captain
- You will likely have many opportunities to work directly with Navy, Marine, and other military officers and enlisted personnel
- Many of our processes are based on military instructions, regulations or practices
- Military names and acronyms pervade our work vocabulary
- When working on ships, there is an expectation that civilians know some basic things about ship life, terms and customs
- The military traditions and ceremonies are very powerful and motivating - civilians are expected to be familiar with them

Three Categories of Military Personnel



- **Officers** – Are commissioned by the President and are highly educated, specially trained military leaders who manage the Navy's personnel, ships, aircraft, and weapons systems.
- **Warrant Officers** – Specialists in their fields who are selected for positions between the ranks of officer and enlisted personnel (US Air Force does not have these)
- **Enlisted** – Those who enlist in the service as non-officers and who perform the numerous specialized tasks that accomplish the mission

Officers

Officers are generalists trained to make decisions and lead organizations of various levels of responsibility and complexity.

In the Navy

- O-1 through O-4 are junior grade officers
- O-5 and O-6 are senior officers
- O-7 through O-10 are flag officers

In the Marine Corp

- O-1 through O-3 are company grade officers
- O-4 through O-6 are field grade officers
- O-7 through O-10 are general officers

In the civilian leadership structure of the United States military, the Marine Corps is a component of the United States Department of the Navy (DoN).
In the military leadership structure, the Marine Corps is a separate branch.

Navy and Marine Corps Officer Titles



In the Navy

- O-1 Ensign (ENS)
- O-2 Lieutenant Junior Grade (LTJG)
- O-3 Lieutenant (LT)
- O-4 Lieutenant Commander (LCDR)
- O-5 Commander (CDR)
- O-6 Captain (CAPT)
- O-7 Rear Admiral Lower Half (RDML) – 1 star
- O-8 Rear Admiral Upper Half (RADM) – 2 star
- O-9 Vice Admiral (VADM) – 3 star
- O-10 Admiral (ADM) – 4 star
- None – Fleet Admiral (Wartime Only)

In the Marine Corps

- O-1 2ND Lieutenant (2nd Lt.)
- O-2 First Lieutenant (1st Lt.)
- O-3 Captain (Capt.)
- O-4 Major (Maj.)
- O-5 Lieutenant Colonel (Lt. Col.)
- O-6 Colonel (Col.)
- O-7 Brigadier General ((Brig. Gen.)
- O-8 Major General (Maj. Gen.)
- O-9 Lieutenant General (Lt. Gen.)
- O-10 General (Gen.)

For a complete chart comparing officer ranks of all service branches, visit the [US DoD Military Officer Rank Insignia Website](#)



How to Interact with Senior Officers

As you may interact with senior officers, generally O-6s and higher, below are some protocols to observe:



- At most military installations, stand for Flag Officers and Commanding Officers (CO) when they enter a room or are announced
- Generally, they are an O-6 or higher (Navy Captain or other Service Branch Colonel)
- Sometimes they are announced before entering the room: “Officer on Deck!”
- A salute is not necessary; civilians do not salute
- Officers and CO’s avoid fraternization with enlisted sailors and soldiers – civilians may generally follow suit when in the presence of officers
- Use sir or ma’am when appropriate
- Use proper military speak when discussing common terms such as dates, time or ship terminology
- Adhere to strict standards of timeliness and appearance when you are expecting to meet with a senior officer

Navy Enlisted Titles

In the Navy

- E1 – Seaman Recruit
- E2 – Seaman Apprentice
- E3 – Seaman
- E4 – Petty Officer 3rd Class
- E5 – Petty Officer 2nd Class
- E6 – Petty Officer 1st Class
- E7 – Chief Petty Officer
- E8 – Senior Chief Petty Officer
- E9 – Master Chief Petty Officer or
- E9 – Fleet or Command Master Chief Petty Officer
- E9 – Master Chief Petty Officer of the Navy



Can be addressed as Petty Officer or by their rate.
E.g., OS1 for an Operational Specialist First Class
Petty Officer.

Can be addressed as Chief, Senior Chief or
Master Chief or by their rate. E.g., ETCS for
an Electronics Technician Senior Chief.

Rate – The pay grade a person works in

Rating – The specialized field the person trains in or works in

Enlisted Navy personnel do not have a rank, only naval officers do

For a complete chart comparing enlisted rates and ranks of all service branches, visit the [US DoD Military Enlisted Rank Insignia Website](#)



USMC Enlisted Titles

In the Marine Corps

- E1 – Private
- E2 – Private First Class
- E3 – Lance Corporal
- E4 – Corporal
- E5 – Sergeant
- E6 – Staff Sergeant
- E7 – Gunnery Sergeant
- E8 – Master Sergeant or First Sergeant
- E9 – Sergeant Major
- E9 – Master Gunnery Sergeant
- E9 – Sergeant Major of the Marine Corps



Rate – The pay grade a person works in

Military Occupational Specialty (MOS) – The specialized field the person trains in or works in (very similar to Navy Rating)

For a complete chart comparing enlisted rates and ranks of all service branches, visit the [US DoD Military Enlisted Rank Insignia Website](#)



Non-Commissioned Officers



Navy Petty Officers and USMC Corporals and Sergeants are considered non-commissioned officers (NCOs) (E4 and higher)

Junior NCOs (E4s) function as first tier supervisors and technical leaders

NCOs serving in the top three enlisted grades (E-7, E-8, and E-9) are termed senior NCOs

- Chief Petty Officers in the Navy (and Coast Guard)
- Expected to exercise leadership at a more general level
- Lead larger groups of service members
- Mentor junior officers, and advise senior officers on matters pertaining to their areas of responsibility
- Marine Corps senior NCOs are referred to as Staff NCOs
- A select few senior NCOs serve at the highest levels of their service, advising their service Secretary and Chief of Staff on all matters pertaining to the well-being and utilization of the enlisted force



Navy Terminology

You may hear or be exposed to various Naval terms, particularly if you work with actual ships or people from shipyards. Here are some terms you will want to be familiar with. Many were derived from hundreds of years of naval operations across the globe.

Hull – The outside part of the ship that rides in or above the water line but below the main deck

Bow or Fore – Forward most part of the hull

Aft or Fantail – Back most part of the hull

Keel – The foundation of the ship, it is the very bottom most part of the hull and it usually forms a V or U shape

Stem – The forward most end of the keel

Stern – The after most end of the keel to which the rudder is usually attached

Bulkheads – The walls in the interior of the ship that divide it into compartments

Decks – Floors of the ship

Portholes – Windows of the ship



USS Constitution – “Old Ironsides”

Navy Terminology

You may hear or be exposed to various Naval terms, particularly if you work with actual ships or people from shipyards. Here are some terms you will want to be familiar with. Many were derived from hundreds of years of naval operations across the globe.

Gangway – Walkway between the shore and the ship used for crew and passengers to board or leave

Go Aloft – Climb up ladders to go to higher decks in the ship

Go Below – Climb down ladders to get to lower decks.

Passageway – Essentially a walkway or hallway leading to other compartments.

Quarterdeck – Not actually a deck, but a designated compartment where official business and operations of the ship are carried out.

Starboard Side – Right hand side of the ship (looking towards the bow)

Port Side – Left hand side of the ship



USS Constitution in dry-dock during restoration/maintenance

Navy Terminology

Applying ship terminology to buildings is very common. Dam Neck site employees checked in at the Quarterdeck this morning. These terms are also used frequently at the Pentagon or the Washington Navy Yard (WNY).

Quarterdeck – Receptionist desk and area

Decks – Floors in a building

Head – Bathroom

Passageways or P-ways – Hallways

Bulkheads – Walls



Washington Navy Yard

Riding a Ship

You may be assigned at some time to visit a ship to see the technology or system your are working on firsthand. Always remember the Ship is the Sailor's home, and you are an onboard guest. It is therefore important to observe and respect the Navy's customs and courtesies, and to always conduct yourself in a professional manner.

All NSWCCD employees planning to ride a ship will undergo shipboard training to learn the etiquette, safety, and procedures aboard ship.



Manning the Rails - A form of salute or honor; in this case, celebrating return to port

Phonetic Alphabet

Aboard ships, signals are sent to one another as letters and/or numbers, which have meanings by themselves or in certain combinations. In the Allied Signals Book, "BZ" or "Bravo Zulu" means "Well Done"

Phonetic Alphabet

Alpha	November
Bravo	Oscar
Charlie	Papa
Delta	Quebec
Echo	Romeo
Foxtrot	Sierra
Golf	Tango
Hotel	Uniform
India	Victor
Juliet	Whiskey
Kilo	X-Ray
Lima	Yankee
Mike	Zulu

Change of Command Ceremony

- The formal passing of responsibility, authority, and accountability of command from one officer to another
- Rich in naval tradition and quite formal
- The relieving orders are read and the outgoing Commanding Officer has the opportunity to say goodbye. The new Commanding Officer reads the order of assignment to command and officially “reports for duty”
- Generally happens about every 3 years at NSWC Carderock.



Daily Honoring of the Colors

- Colors are honored every day at 0800 and sunset
- If you observe that this ceremony is about to begin, follow these guidelines:
 - If driving, pull over and wait for the ceremony to conclude
 - If walking, stop, face the direction of the flag or music, and cover your heart with your right hand until the ceremony is concluded



Ceremonial Honoring of the Colors at Events

- A Color Guard will move forward with the Flags to present to all people present
- All present rise and face the Color Guard
- The National Anthem is played
- At this time, all military members salute while the music plays
- All civilians remove their hats and place their right hand over their hearts



The Flag may be referred to as: “The Flag”,
“The Colors”, “The Standard” or
“The National Ensign”

Recognition by the CO or Executive

Navy employees can receive recognition from the CO or an Executive from NSWCCD or another military activity for a job well-done



- A formal letter of recognition may be sent
- A formal awarding of honor or recognition in the correct venue may take place, e.g.:
 - A department technical award
 - A NSWCCD award at the annual awards ceremony

In Closing...



These are just some of the interesting facets of Navy and Military protocol.

For more information on Navy Protocol, you can research several Navy and commercial websites.

Here are a few suggestions:

Official Site of the United States Navy – www.navy.mil

Official website of the Department of Defense – www.defense.gov

Naval History and Heritage Command – www.history.navy.mil



Command Evaluation and Review Office (Code 00N)



Command Review & Investigations Office



Staffing:

- Duc Cang, Acting CR&I Director/Investigator
- Vacant, Auditor
- Vacant, Investigator



NSWCCD Instruction 5000.1D

- Command Review & Investigations Program
- CR&I is meant to provide the Commanding Officer (CO) with an independent, in-house assessment capability designed to assist in improving mission accomplishment, integrity of command and economical use of resources. command or activity operations. The CR&I Office is a staff function that reports directly to the CO.

Programmatic Functions:

1. Hotline Program (Fraud, Waste, Abuse & Mismanagement)

- Serves as the focal point for FWA matters, including overall program coordination.
- Conducts investigations and inquiries of internal/ external hotline allegations.
- If appropriate, refers fraudulent cases to Naval Criminal Investigative Service.

2. Command Directed Investigations (CDIs)

- Conducts Management Inquiries, Preliminary Inquiries, JAGMAN investigations and other Command-level Investigations as directed by the Commanding Officer.

3. Command Evaluations/Reviews (Annual Plan)

- Conducts periodic and special reviews, evaluations, studies and analyses of command or activity operations.
- Provides an independent, in-house capability to detect deficiencies, improprieties or inefficiencies.
- Provides recommendations to correct conditions which adversely impact mission accomplishment, command integrity, or efficient use of resources.

4. Audit Liaison/Follow-up

- Serves as Division liaison, and provides logistical and administrative support for the GAO, NAVAUDSVC, DOD IG, and NAVINSGEN.
- Maintains a central depository of audit reports and audit responses to findings and recommendations.

Matters Appropriate for the Inspector General's Hotline

- * Abuse of Title/Position
- * Bribes/Kickbacks/Acceptance of Gratuities
- * Conflicts of Interests
- * Ethics Violations
- * False Official Statements/Claims
- * Fraud
- * Gifts (Improper receipt or giving)
- * Waste (Gross)
- * Misuse of Official Time, Gov't Property, Position and Public Office
- * Political Activities
- * Purchase Card Abuse
- * Reprisal (Military Whistleblower Protection)
- * Safety/Public Health (Substantial/Specific)
- * Systemic Problems
- * Time and Attendance (Significant Violations)
- * Travel Card Abuse/Travel Fraud
- * Mismanagement/Organ. Oversight (Significant Cases)



QUESTIONS?

REMEMBER THE HOTLINE NUMBER: (301) 227-4228

Visit our Intranet Site:

<https://cuthill.aw3s.navy.mil/intra/ig/>

How to File a Complaint:

https://cuthill.aw3s.navy.mil/intra/ig/how_to_file.html

NAVSEA Hotline Number: 1-800-356-8464

NAVSEA Hotline Email: NSSC_NAVSEAIGHotline@navy.mil

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



NSWCCD STEM & Outreach

Charlotte George, STEM and Outreach Program Director

(301) 227-8869, charlotte.george@navy.mil

CAPT Todd Hutchison

Commanding Officer, NSWCCD

Larry Tarasek

Technical Director (Acting), NSWCCD

January 30, 2019

STEM & Outreach Program

Naval STEM Strategy

NSWCCD supports a broad range of educational outreach programs, with the long term goal of building a relevant and capable future STEM workforce, by strengthening the STEM workforce pipeline through Outreach.

Our initiatives aim to:

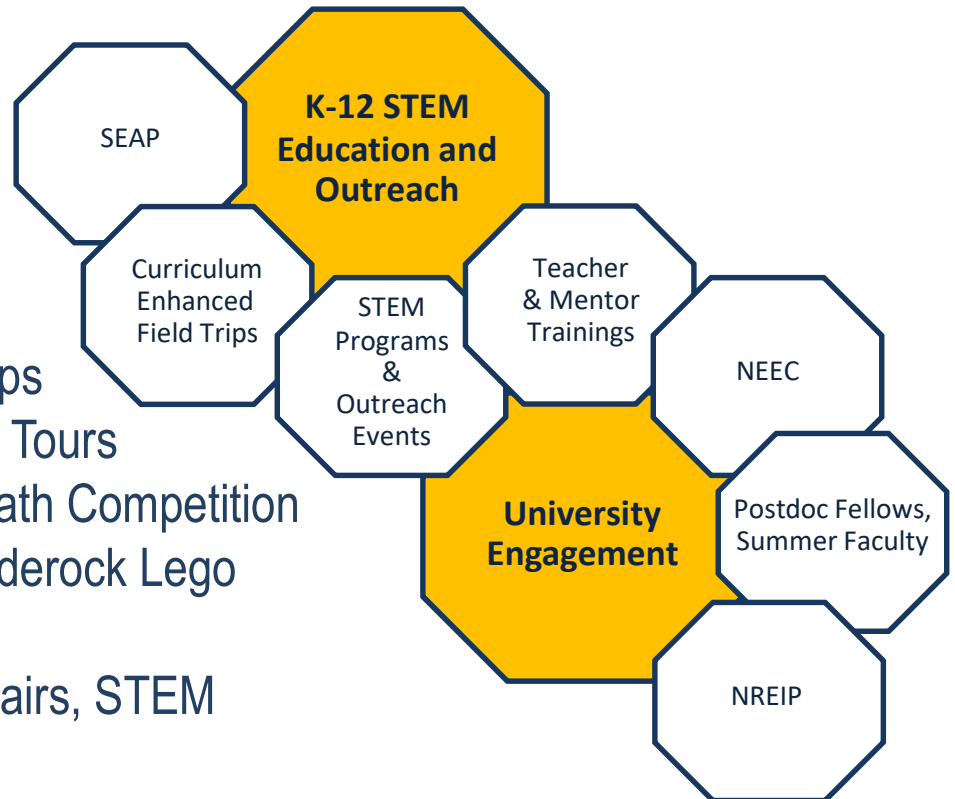
- **INSPIRE** student interest in STEM through hands-on, accessible applications of naval STEM fundamentals
- Provide practical experiences to **ENGAGE** students and teachers of all ages to "learn by doing"
- **EDUCATE** the next generation with foundational skills and knowledge needed to pursue advanced STEM education and careers



* Above Graphic from 2018
Naval STEM Strategy

STEM & Outreach Efforts

- The SeaPlane Program
- The SeaPerch Program
- The SeaGlide Program
- The International Submarine Races
- NSWCCD Summer Institute for Educators
- High School and University/College Internships
- Curriculum Enhanced Field Trips and Facility Tours
- MathCounts Mentoring and the Carderock Math Competition
- FIRST Lego Robotics Mentoring and the Carderock Lego Challenge
- STEM Event Support (Career Days, STEM Fairs, STEM Competitions, etc.)



AMERICA'S FLEET STARTS HERE

Contact Information



- **Charlotte George, *STEM & Outreach Director***
 - charlotte.george@navy.mil
- **Haley Kirby, *STEM & Outreach Coordinator***
 - haley.kirby@navy.mil
- **Rachel Luu, *Intern Coordinator***
 - rachel.luu@navy.mil

Questions

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



New Hire Bridge

CAPT Todd Hutchison
Commanding Officer, NSWCCD

January 30, 2019

Larry Tarasek
Technical Director (Acting), NSWCCD

New Hire Bridge

The New Hire Bridge (NHB) is a network of employees who started within the last 5 years at the Naval Surface Warfare Center Carderock Division (NSWCCD). Please use this site to transition into your new career and acquaint yourself with the activities at Carderock.



Past Events



Past Events

- Lunches
- Happy Hour's
- Hockey Games
- Baseball Games
- Hiking
- Pumpkin Picking
- Early Career Development Series
- ETC.

Open Positions

- Social Chair
- Programs Chair
- Website Chair

Contact Information



- **Daniel Gallutia, *Chair***
 - daniel.gallutia1@navy.mil
 - 227-1747
- **Kelley Stirling, *Co-Chair***
 - kelley.stirling@navy.mil
 - 227-8833
- **Haley Kirby, *Secretary***
 - haley.kirby@navy.mil
 - 227-8843
- **Krista Michalis, *Champion***
 - krista.michalis@navy.mil
 - 227-4342

Questions

Break 1



Break 1



Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



NSWCCD Initial Security Orientation Briefing



Vicky Davis, Security Policy and Programs (Code 1051)

Captain Todd E. Hutchison

Commanding Officer, NSWCCD

Larry Tarasek

Technical Director, NSWCCD



Security Education & Awareness



‘Activities undertaken to ensure that people have the skills, knowledge, and information to enable quality performance of security functions and responsibilities, **understand** security program policies and requirements, and **maintain continued awareness** of security requirements and intelligence threats.’



Security Mission

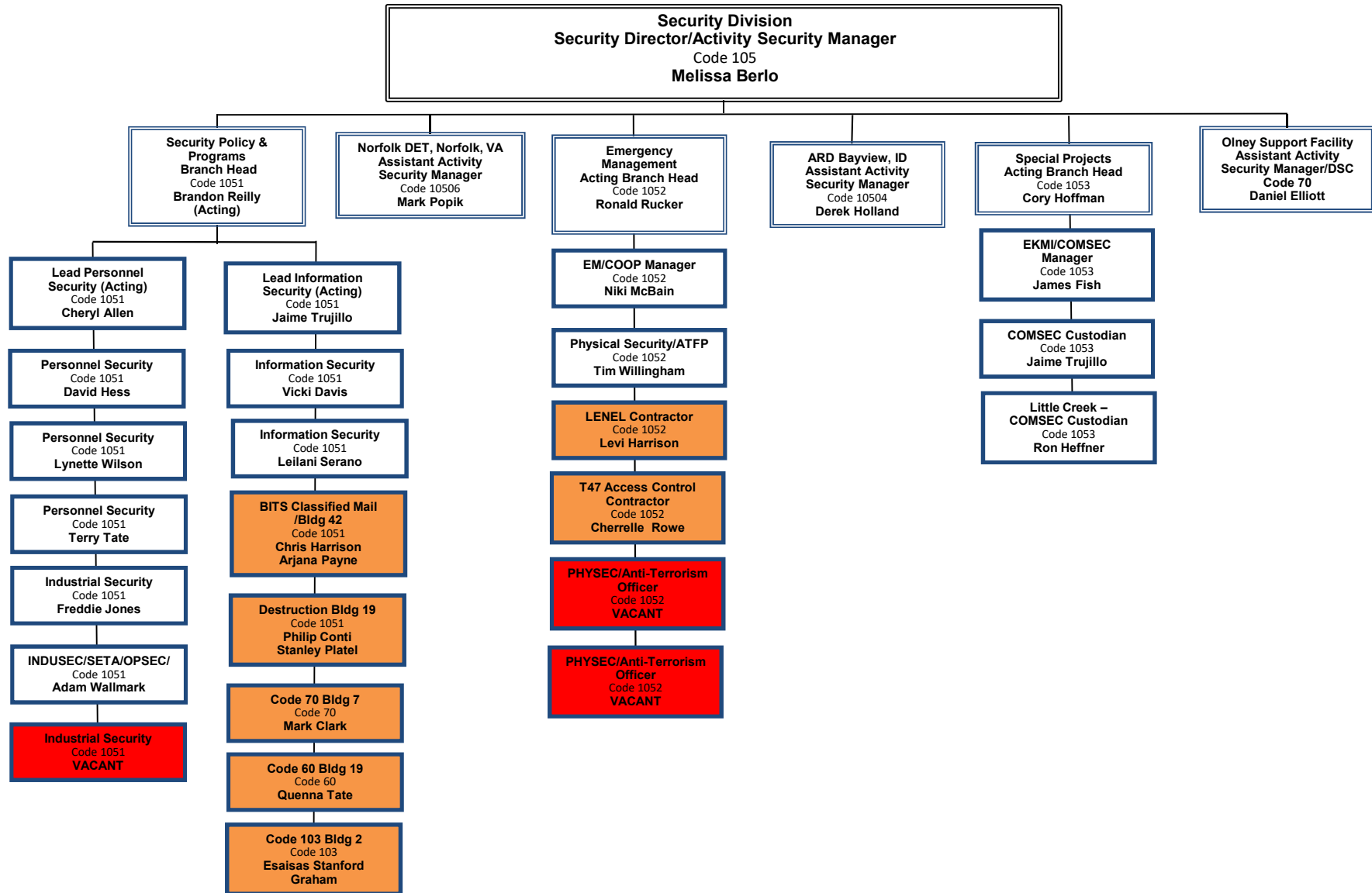
The protection of U.S. Government assets including people, property, and both classified and controlled unclassified information is the responsibility of each and every member of the Department of Navy (DON), regardless of how it was obtained or what form it takes. **Our vigilance is imperative.** Anyone with access to these resources has an obligation to protect them.



Objectives

- Identify each functional areas and responsibilities of security
- Provide a basic understanding of DOD, SECNAV, NAVSEA and Carderock security policies

Security Division (Code 105)



Code 105 Security Office Hours



Building 42, 1st Floor, Room 100/104

301-227-1408/Multiple Group Mailboxes

Main Hours: 0730-1600

- **Services:**
- 0730 – 1500
 - Classified Mail Handling/Document Control
 - Courier Cards
 - CAC Access
 - Check in/Check out
 - FedEx Drop Offs - NLT Noon, prior day
 - Last day/time for pick up - Thursday by 0900

Personnel Security

Security Clearances

- Employment with the NSWCCD requires you to maintain eligibility for access to classified information
- Completed Electronic Questionnaires for Investigation Processing (e-QIP) system
- Access to classified information will be authorized at the level necessary to perform your duties

Eligibility for Access to Classified Material is a privilege, not a right.

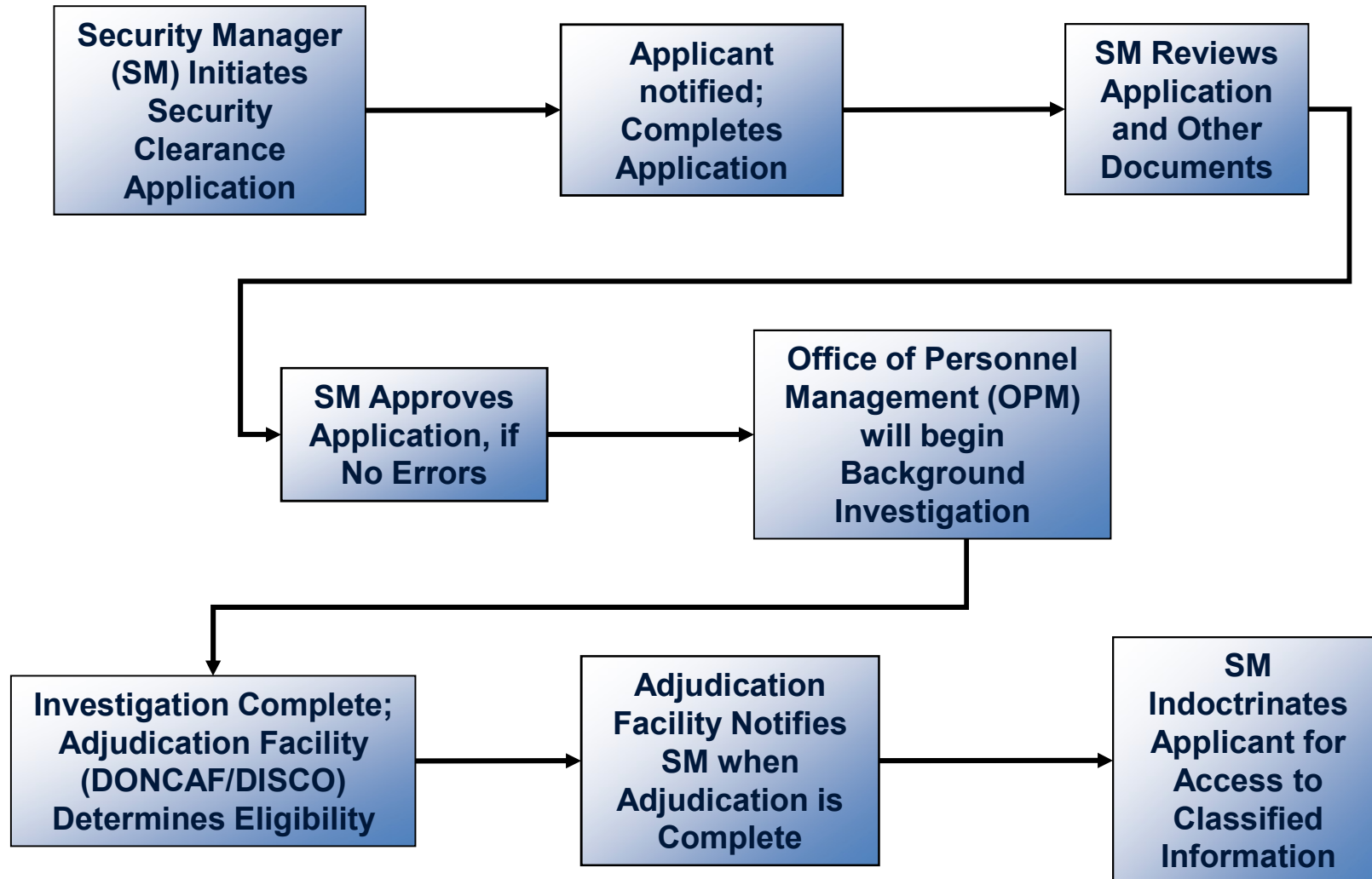




Your Security Clearance

- Position sensitivity and/or duties will determine level of clearance or access
- There are three levels of Security Access Requirements (SAR):
 - Top Secret (TS)
 - Secret (S)
 - Confidential (C)
- You **MUST** coordinate with your Security Manager for all matters concerning security clearance/access!

Security Clearance Process



13 Adjudicative Guidelines

A - Allegiance to the U. S.
B - Foreign Influence
C - Foreign Preference

ALLEGIANCE ISSUES

D - Sexual Behavior
E - Personal Conduct
F - Financial Considerations

CHARACTER ISSUES

G - Alcohol Consumption
H - Drug Involvement & Substance Abuse
I - Psychological Conditions

HEALTH ISSUES

J - Criminal Conduct
K - Handling Protected Information
L - Outside Activities
M - Use of Information Technology

BEHAVIOR ISSUES



Access Eligibility Process

Eligibility Determination

Administrative action, usually involving a form of background investigation and adjudication determination for trustworthiness



SF 312

Classified Information Nondisclosure Agreement: All persons authorized access to classified information are required to sign a SF 312, a legal contractual agreement between you and the U.S. Government.



Need-to-Know

Determination made by an authorized holder of classified information that a prospective recipient requires access to perform a lawful and authorized government function.



Access

The ability and opportunity to obtain knowledge of classified information.



Continuous Evaluation Program



Employees must recognize and avoid behaviors that might jeopardize their security clearance.

In accordance with NSWCCD Policy Statement for Continuous Evaluation Program, dated 22 FEB 17: individuals are required to report to their supervisor or appropriate security personnel and seek assistance for any incident or situation that could affect their continued eligibility for access to classified information. Individuals shall be initially and periodically briefed thereafter, to ensure familiarity with pertinent security regulations and the standards of conduct required of individuals holding positions of trust.

*****The ultimate responsibility for maintaining eligibility to access classified information rests on YOU!*****

Self-Reporting

Self-reporting is mandatory and emphasizes personal integrity

With this privilege comes the obligation to report certain activities

Foreign Travel



Foreign Contacts



Marriage/Divorce



Alcohol Abuse



Drug Use



Bankruptcy/ Credit Issues



Incarceration/ Arrest



Foreign Allegiance



Loss/Compromise of Classified Info



*Foreign Influence

**Foreign Ownership, Control or Influence (FOCI) concerns*



Classified Info Non-Disclosure



SF-312, Classified Information Nondisclosure Agreement

- Full Name
- SSN
- Signature
- Witness
- Debriefing
- Lifetime

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT			
AN AGREEMENT BETWEEN		AND THE UNITED STATES	
<small>(Name of Individual - Printed or typed)</small>			
<p>1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.</p> <p>2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.</p> <p>3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.</p> <p>4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, "652 and 1924, title 18, United States Code, "the provisions of section 783(b), title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1962; recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.</p> <p>5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.</p> <p>6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.</p> <p>7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information, if I do not return such materials upon request. I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.</p> <p>8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.</p> <p>9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.</p> <p>10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information; (2) communications to Congress; (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.</p>			
<small>(Continue on reverse.)</small>			
<small>NON 1545d-1280-6489 Previous edition not usable.</small>		<small>STANDARD FORM 312 (Rev. 7-2013) Prescribed by GONI 32 CFR PART 2001.90 E.O. 13526</small>	
<p>11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 7071) or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1962 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an Inspector General); the Inspector General of the Intelligence Community, and Congress; section 1033(g)(3) of the National Security Act of 1947 (50 U.S.C. 4033(g)(3)) (relating to disclosures to the Inspector General of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 4033(d)(5) and 4033(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, "652 and 1924 of title 18, United States Code, and section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.</p> <p>12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001 - section 2001.90(e)(2)) so that I may read them at this time, if I so choose.</p>			
<small>*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.</small>			
<small>SIGNATURE</small>		<small>DATE</small>	
<small>SOCIAL SECURITY NUMBER (See Notice below)</small>			
<small>ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)</small>			
<small>WITNESS</small>		<small>ACCEPTANCE</small>	
<small>THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.</small>		<small>THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.</small>	
<small>SIGNATURE</small>		<small>SIGNATURE</small>	
<small>DATE</small>		<small>DATE</small>	
<small>NAME AND ADDRESS (Type or print)</small>		<small>NAME AND ADDRESS (Type or print)</small>	
<small>SECURITY DEBRIEFING ACKNOWLEDGEMENT</small>			
<p>I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information; and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.</p>			
<small>SIGNATURE OF EMPLOYEE</small>		<small>DATE</small>	
<small>NAME OF WITNESS (Type or print)</small>		<small>SIGNATURE OF WITNESS</small>	
<p><small>NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-194 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.</small></p>			
<small>STANDARD FORM 312 BACK (Rev. 7-2013)</small>			

FRONT

BACK

NOTE: Contractors Only - fill out organization information

Information Security

Information Security

The protection of classified and controlled unclassified information (CUI), including but not limited to:

- Marking
- Handling
- Transmission
- Storage
- Destruction



Information Categories

■ Classified Information

- **TOP SECRET (TS)** (Exceptionally Grave Damage)
- **SECRET (S)** (Serious Damage)
- **CONFIDENTIAL (C)** (Damage)

■ Controlled Unclassified Information

- For Official Use Only (FOUO) [FOIA exemptions 2-9]
- Distribution Controlled
- Personal Identifiable Information (PII)
- Privacy Act Information
- Proprietary Information (ownership belongs to Contractor)



Safeguarding Classified Information

Cover Sheets

SF 703 - Top Secret (orange)

SF 704 - Secret (red)

SF 705 - Confidential (blue)



Labels

SF-706 - Top Secret (orange)

SF-707 - Secret (red)

SF-708 - Confidential (blue)

SF-709 - Classified (purple)

SF-710 - Unclassified (green)



Types of Classified Materials

Classified Material can include **ANY** of these and must be properly marked:



Machinery, Documents
Emails, Models, Faxes
Photographs, Reproductions
Storage Media, Working Papers, Meeting
Notes, Sketches, Maps, Products,
Substances,
or Materials

How Information Is Classified?

■ Original Classification

- Initial classification decision
- Original Classification Authority (OCA)
 - Designated in writing by SECNAV (for Top Secret) and DUSN (Policy) (for Secret)
 - **NOTE: Commanding Officer, NSWC Carderock Division IS NOT an OCA**

■ Derivative Classification

- Incorporating, paraphrasing, restating, or generating, in new form, information that is already classified
- **Training is mandatory every year!**
- Derivative sources:
 - Security Classification Guide (SCG)
 - Properly marked source documents (e.g., books, pamphlets, etc.)
 - DD Form 254, DoD Contract Security Classification Specification

Classified Information Source Lines



ORIGINAL CLASSIFIER

*Classified By: John Smith, Director
Reason: 1.4(c)
Declassify On: 20551231*

DERIVATIVE CLASSIFIER

*Classified By: Sue Jones, Code 453
Derived From: PMO Ships SCG
Declassify On: 20551231*

Handling Classified Information

Must be:

- Under positive control by an authorized person and/or stored in an approved GSA container, vault, or secure room
- Discussed only in authorized areas and/or processed via authorized systems/equipment (e.g., STE, SIPRNet, JWICS)
- Protect/safeguard with appropriate cover sheet
- Properly marked
- Must have a courier card when hand carrying
- Secured/protected when found unattended

Storing Classified Information

■ Classified Information Must Be:

- In a GSA Approved Container/Secure Room/Vault when not being used

■ DO NOT:

- Leave classified material unattended
- Leave classified material in desk drawers
- Leave classified material in open security containers

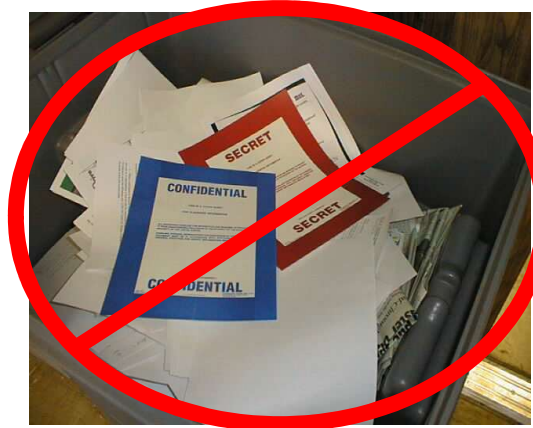


*****DO NOT TAKE CLASSIFIED MATERIAL HOME*****

Destruction of Classified Information

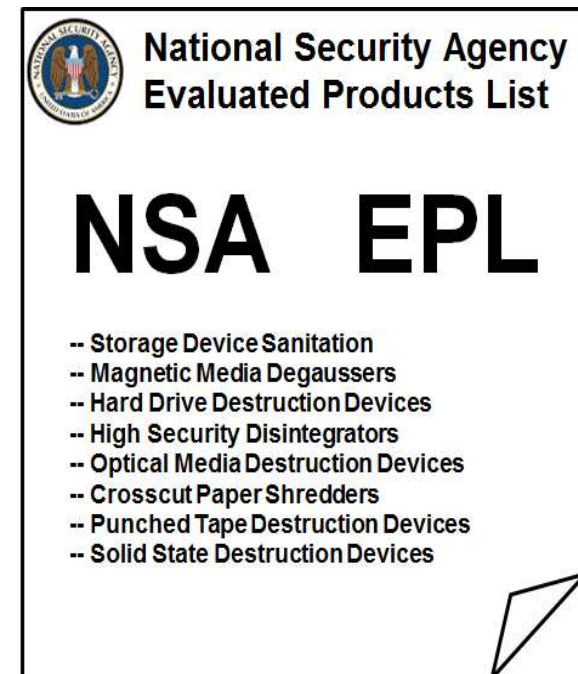
- Must be destroyed in device approved for classified material destruction*
- Approved shredders are located throughout the Command
- Shredders will contain a certification memo
- Other classified media – Contact Security (227-1408)
- All NNPI must be destroyed via approved methods*
- All purchases of classified information destruction devices must be coordinated through Security (Code 105)

**Destruction device must be listed on a current NSA Evaluated Products List (EPL)*



Destruction of Classified Information

- Burning
- Shredding*
- Pulverizing*
- Disintegrating*
- Degaussing*
- Pulping
- Melting
- Chemical Decomposition
- Mutilation



**NSA/CSS Evaluated Products List (EPL)*

Incident Categories Defined

Willful

Negligent

Inadvertent

- An incident is **willful** if the person purposefully disregards DoD security or information safeguarding policies or requirements (e.g., intentionally bypassing a known security control).
- An incident is **negligent** if the person acted unreasonably in causing the spillage or unauthorized disclosure (e.g., a careless lack of attention to detail, or reckless disregard for proper procedures).
- An incident is **inadvertent** if the person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring (e.g., the person reasonably relied on improper markings).

Per DEPSECDEF memo of 14 Aug 2014, Subject: Unauthorized Disclosure of Classified Information or Controlled Unclassified Information on DoD Information Systems

Types of Security Incidents

- **Violations** - Any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.

Examples include:

- Open/unattended security containers
- Discussing classified information in an unsecure setting
- Processing classified information on unclassified systems

(Note: The presence of classified information on the NMCI NIPRNET is always considered a Security Violation).

[Electronic Spillage]

- **Infractions** - Any knowing, willful or negligent action contrary to the requirements of an order or its implementing directives that do not constitute a 'violation', as defined above. Examples include:

- Failure to use a cover sheet
- Not using a security container checklist
- Not using open/closed sign on a security container

Physical Security

Protection and Prevention

The two primary purposes of physical security are **PREVENTION** and **PROTECTION**. Properly designed and executed physical security programs should deter or prevent to the greatest degree possible the loss, theft, or damage to an asset.

Protection of:

- Resources
- Facilities
- Classified Information
- Operations

Prevention from:

- Theft
- Unauthorized Access
- Loss
- Compromise

Physical Security

Physical security functions offer security-in-depth, and include, but are not limited to:

- Perimeter fences
- Employee and visitor access controls
- Badges/Common Access Cards (CAC)
- Intrusion Detection Systems (IDS)
- Random guard patrols
- Prohibited item controls
- Entry/Exit inspections
- Visitor escorts
- CCTV monitoring



Storing Classified Information

- Custodian responsibilities
- Container maintenance
- Combo changes
- SF-700, Security Container Info
- SF-701, End of Day Checklist
- SF-702, Security Container Checklist

GSA



SF 700 Security Container Information

- Initiate a combination change when an employee no longer requires access, if there is a compromise, and/or when a container is placed in/out of service.
- Fill out page one and place in an opaque envelope
 - Lists after-hours custodian contact information (PII)
 - Place sealed envelope in control drawer of security container
 - Page two lists combo, place in sealed envelope and provide to Security Office

FOR OFFICIAL USE ONLY

SECURITY CONTAINER INFORMATION INSTRUCTIONS		1. AREA OR POST (if required)	2. BUILDING (if required)	3. ROOM NO.
1. Complete Part 1 and Part 2A (on end of flap). 2. Detach Part 1 and attach to the inside of the control drawer of the security container. 3. Mark Parts 2 and 2A with the highest classification level stored in this security container. 4. Detach Part 2A, insert in envelope (Part 2) and seal. 5. See Privacy Act Statement on reverse.		NSWCCD	42	104
		4. ACTIVITY (Division, Branch, Section or Office)		5. CONTAINER NO.
		Code 1051		1046 SF
		6. MFG. & CLASS OF CONTAINER	7. MFG. & LOCK MODEL	8. SERIAL NO. OF LOCK
		Mosier	X-07	N/A
9. DATE COMBINATION CHANGED	10. PRINT NAME/ORGANIZATION SYMBOL WITH SIGNATURE OF PERSON MAKING CHANGE			
05/29/2018	Matthew Stubblefield Code 1051 <i>Matthew Stubblefield</i>			
11. Immediately notify one of the following persons, if this container is found open and unattended.				
EMPLOYEE NAME		HOME ADDRESS		HOME PHONE
Matthew Stubblefield		Complete Address		Complete phone number
Timothy Willingham		Complete Address		Complete phone number

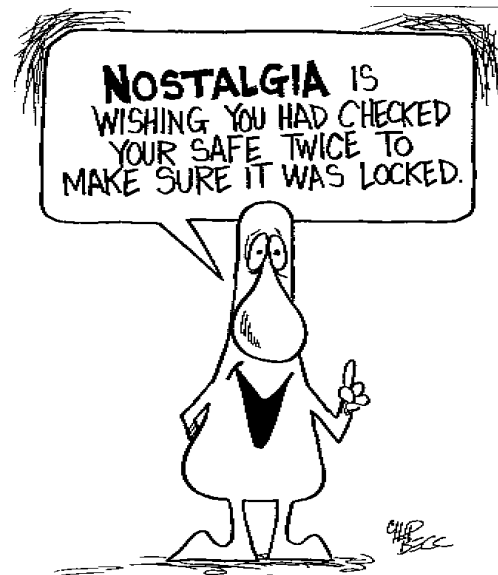
1. ATTACH TO INSIDE OF SECURITY CONTAINER

700-102
NSN 7540-01-214-5372

STANDARD FORM 700 (REV. 4-01)
Prescribed by NARA/ISOO
32 CFR 2003

Security Containers and Secure Rooms

- SF 702-Security Container Check Sheet
 - Posted on outside of container or door
 - Every day must be accounted for including weekends and holidays
 - Completed form retained for 90 days from last entry



SECURITY CONTAINER CHECK SHEET								
FROM	ROOM NO.	BUILDING	CONTAINER NO.					
	151	55	HV-321					
CERTIFICATION								
I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.								
MONTH/YEAR								
May 2017								
DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME
1	MJS	0600	MJS	0830	MJS	1600		
2	MJS	0630	MJS	0800				
	MJS	1000	MJS	1400	MJS	1600		
3	MJS	0630	MJS	0830				
	MJS	1100	MJS	1130				
	MJS	1500	MJS	1530	HJP	1600		
4	NOT OPENED				MJS	1600		
5	MJS	0600	MJS	1400	HJP	1600		
6	WEEKEND							
7	WEEKEND							
8	MJS	0700	MJS	1200	HJP	1600		
9	MJS	0730	MJS	1500	HJP	1600		
10	MJS	0530	MJS	0700				
	MJS	0900	MJS	1100				
	MJS	1200	MJS	1300				
	MJS	1330	MJS	1500	MJS	1500		
11	TDY							
12								
13								
14								
15	MJS	0600	MJS	1500	MJS	1500		
16	NOT OPENED				MJS	1600		

End-of-Day Security Checks

- SF 701-Activity Security Checklist
 - Posted on inside of room, closest to exit
 - Annotate weekends and holidays
 - Completed form retained for 90 days from last day

ACTIVITY SECURITY CHECKLIST		DIVISION BRANCH OFFICE Code 99 (Bldg. 55)		ROOM NUMBER 151		MONTH AND YEAR May 2017																									
Irregularities discovered will be promptly reported to the designated Security Office for corrective action.		Statement																													
I have conducted a security inspection of this work area and checked all the items listed below.																															
TO (if required)		FROM (if required)				THROUGH (if required)																									
*ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security container	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	
2. Windows secure	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	
3. Alarms set	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	
4. Interior office doors locked	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	
5. Coffee pot unplugged	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	
6.																															
7.																															
8.																															
INITIAL FOR DAILY REPORT																															
TIME	1600	1600	1600	1600	1600			1600	1600	1600	1600	1600			1600	1600	1600	1600	1600			1600	1600	1600	1600	1600			1600	1600	

Access

- Base Access:
 - Common Access Card (CAC)
 - Authorized pass
 - Defense Biometric Identification System (DBIDS)
 - Credentialing for contractors, vendors, and suppliers requiring recurring access
 - Not required for contractors with CAC
 - All contractors (w/o a CAC), vendors and delivery personnel are required to complete and sign the SECNAV Form 5512/1
 - Credentials require a sponsor



Prohibited Items

These items and those similar in nature are **prohibited** inside NSWCCD Office Spaces

* Photography



Alcohol



Drugs



XXX

Sexually Explicit
Material



Weapons
(Guns/Knives)

* Permission Required

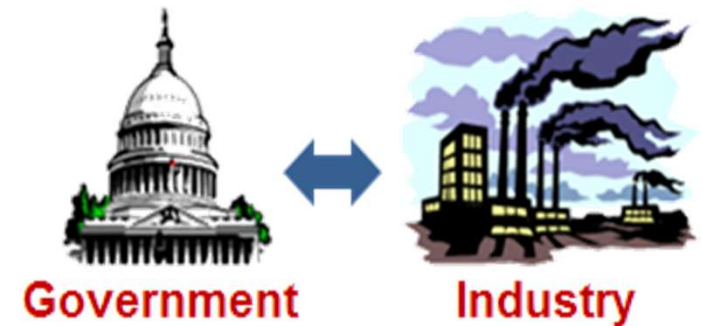
Cell Phones and PED Policy

- **Personally-owned cell phones are prohibited in:**
 - Restricted Areas
 - Open Storage Areas
 - Sensitive Compartmented Information Facilities (SCIF)
 - Explosive operations buildings and storage areas
- **CUI**
 - NAVSEA and Carderock PED Policies in place
 - NAVSEA Update, May 2016: "In such spaces [basic office spaces], sound judgment is required prior to conducting discussions. Although PEDs are authorized in these locations, each employee is responsible to ensure that controlled information is not inadvertently exposed to unauthorized personnel and recording of any kind is prohibited."

Industrial Security

Industrial Security

- A **partnership** between the federal gov't and industry in order **to safeguard classified information**
- Establishes standards for contracting companies who have access to classified information
- Prevents unauthorized disclosure of classified by:
 - Defining requirements
 - Identifying restrictions
 - Establishing safeguards



- Prior to disclosing classified information:
 - Determine if contractor requires access in connection with a legitimate U. S. Government requirement
 - Contract Solicitation
 - Pre-contract Negotiation
 - Contractual Relationship
 - IR&D Effort
 - Determination based on:
 - Facility clearance valid for access at same or lower classification level as FCL
 - Storage capability

DD Form 254

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <small>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</small>		1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED b. LEVEL OF SAFEGUARDING REQUIRED	
		2. THIS SPECIFICATION IS FOR: (X and complete as applicable) a. PRIME CONTRACT NUMBER b. SUBCONTRACT NUMBER c. SOLICITATION OR OTHER NUMBER DUE DATE (YYYYMMDD)	
3. THIS SPECIFICATION IS: (X and complete as applicable) a. ORIGINAL (Complete date in all cases) DATE (YYYYMMDD) b. REVISED (Supersedes all previous specs) REVISION NO. DATE (YYYYMMDD) c. FINAL (Complete item 6 in all cases) DATE (YYYYMMDD)		4. IS THIS A FOLLOW-ON CONTRACT? YES NO. If Yes, complete the following: Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.	
5. IS THIS A FINAL DD FORM 254? YES NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.		6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code) a. NAME, ADDRESS, AND ZIP CODE b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
7. SUBCONTRACTOR a. NAME, ADDRESS, AND ZIP CODE b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)		8. ACTUAL PERFORMANCE a. LOCATION b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT			
10. CONTRACTOR WILL REQUIRE ACCESS TO: YES NO		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: YES NO	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION b. RESTRICTED DATA c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION d. FORMERLY RESTRICTED DATA e. INTELLIGENCE INFORMATION (1) Sensitive Compartmented Information (SCI) (2) Non-SCI f. SPECIAL ACCESS INFORMATION g. NATO INFORMATION h. FOREIGN GOVERNMENT INFORMATION i. LIMITED DISSEMINATION INFORMATION j. FOR OFFICIAL USE ONLY INFORMATION k. OTHER (Specify)		a. HAVE ACCESS TO CLASSIFIED INFORMATION FROM ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT AGENCY b. RECEIVE CLASSIFIED DOCUMENTS ONLY c. RECEIVE AND GENERATE CLASSIFIED MATERIAL d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE e. PERFORM SERVICES ONLY f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S. (PERTAINING TO U.S. POSSESSION AND THROUGH TERRITORIES) g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER h. REQUIRE A COMSEC ACCOUNT i. HAVE TEMPEST REQUIREMENTS j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE l. OTHER (Specify)	

DD FORM 254, DEC 1999

PREVIOUS EDITION IS OBSOLETE.

Reset Adobe Professional 7.0

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify)

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. Yes No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. Yes No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL b. TITLE c. TELEPHONE (include Area Code)

d. ADDRESS (include Zip Code)

e. SIGNATURE

17. REQUIRED DISTRIBUTION

- 1. CONTRACTOR
- 2. SUBCONTRACTOR
- 3. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- 4. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- 5. ADMINISTRATIVE CONTRACTING OFFICER
- 6. OTHERS AS NECESSARY

DD FORM 254 (BACK), DEC 1999

Reset

Other General Security Tasks



Other Key Processes

- Base Access for Visitors
- Hosting Foreign Visitors
- Foreign Travel Process

NSWCCD Visitors

- Major events (e.g., sub races, STEM competition)
 - Visitors are required to complete and sign the SECNAV Form 5512/1
 - Form 5512/1 must be submitted five (5) days prior to visit
- Classified Meetings or other official visits
 - Carderock employee notifies Security Office of visitor
 - Initiate coordination at least 10 days prior to visit
- Upon arrival Visitor must provide name of POC

Hosting Foreign Visitors



■ Official Visits

- Must be processed/approved via Foreign Visit System (FVS)
- Security Division notifies Code sponsor and NCIS (Contact Officer)
- Three types: One time; Recurring; Extended
- Coordinate with NAVSEA HQ if DDL required
- If authorized, visitor can have accessed to classified information

■ Unofficial Visits

- Courtesy calls, general visits, public events, etc.
- Hosting code submits CARDEROCKDIV 5512/6
- Security Division will coordinate with host code and Visitor Center
- No access to classified information is authorized

Foreign Travel

All personnel traveling outside of U.S. on official duty or on leisure must:

- Submit a CARDERDIV Form 5540/1 at least 30 days prior to departure
- Submit a CARDERDIV Form 5540/2 within 3 business days of return to duty

Pre-travel guidance is provided in the Foreign Clearance Guide (<https://www.fcg.pentagon.mil>)

This process ensures the Foreign Travel Brief is given to personnel who require them. The briefs increase awareness regarding:

- Personal Safety
- Potential targeting
- Travel warnings and alerts
- Where to seek assistance



Check-In/Check-Out Procedures



ALL personnel MUST check-in and check-out with the Security Division (Code 105)

- Receive Security Briefings/Debriefings
- Turn in badges, credentials, CACs, ID Cards, etc.
- Receive/Return Courier Cards
- Update JPAS records
- Ensure ALL classified information assigned to you is transferred to the appropriate program/person before check-out
- **Security (Code 105), Bldg. 42 should be the final stop, on the last duty day, before departing the installation.**

Summary

Why are we here?



Ana
Montes



Edward
Snowden



Jerry
Whitworth



Aldrich
Ames



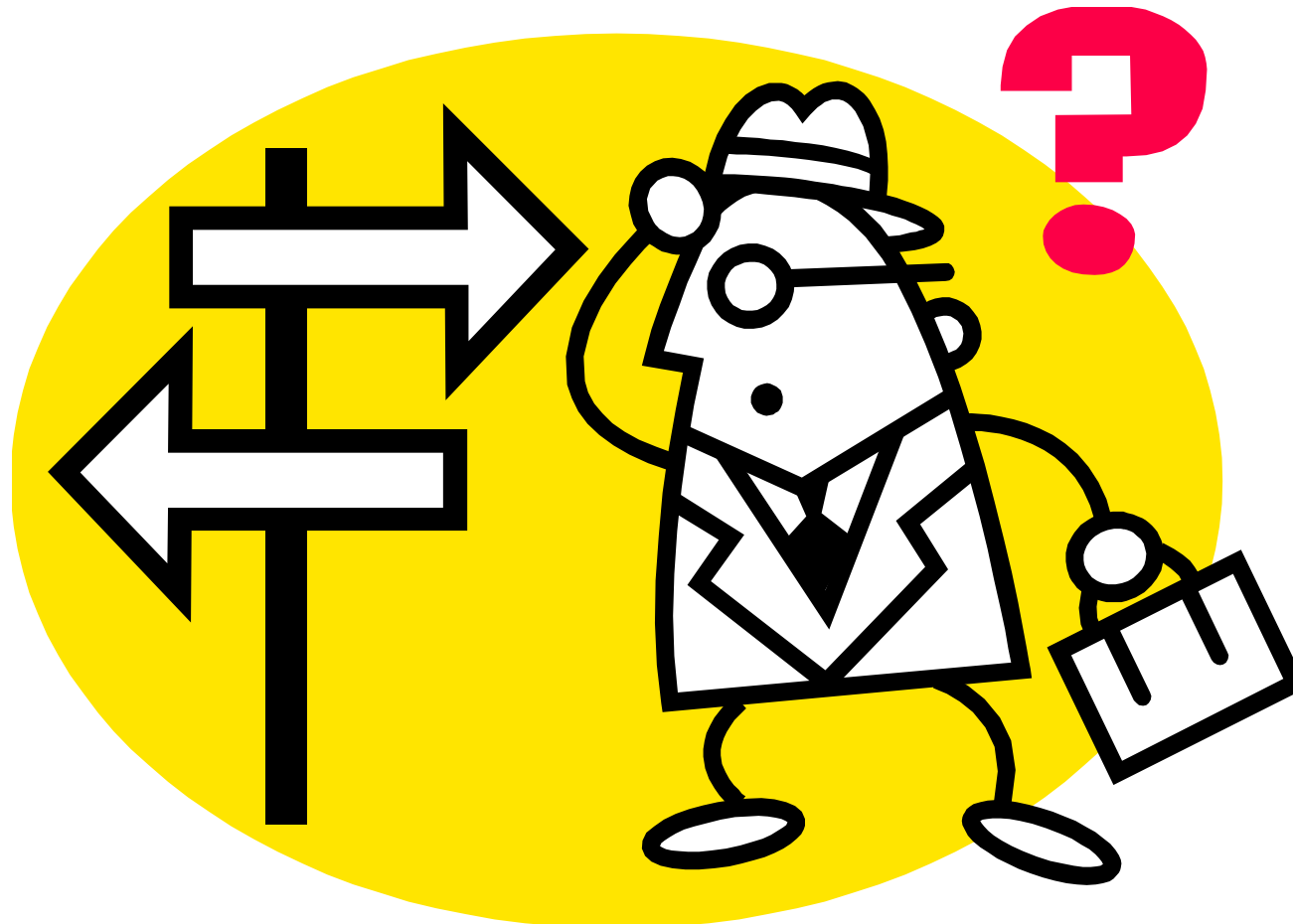
Robert
Hanssen



Bradley
Manning

The importance of security awareness and vigilance on the part of all employees cannot be overemphasized. It helps to detect internal and external threats and vulnerabilities ultimately assisting in preventing security breaches. It is only when all employees are vigilant and aware, that those who disregard security policies and procedures can be identified before causing irreparable damage to national security.

Questions?





Contact Information



Vicky Davis

Security Office (Code 1051)

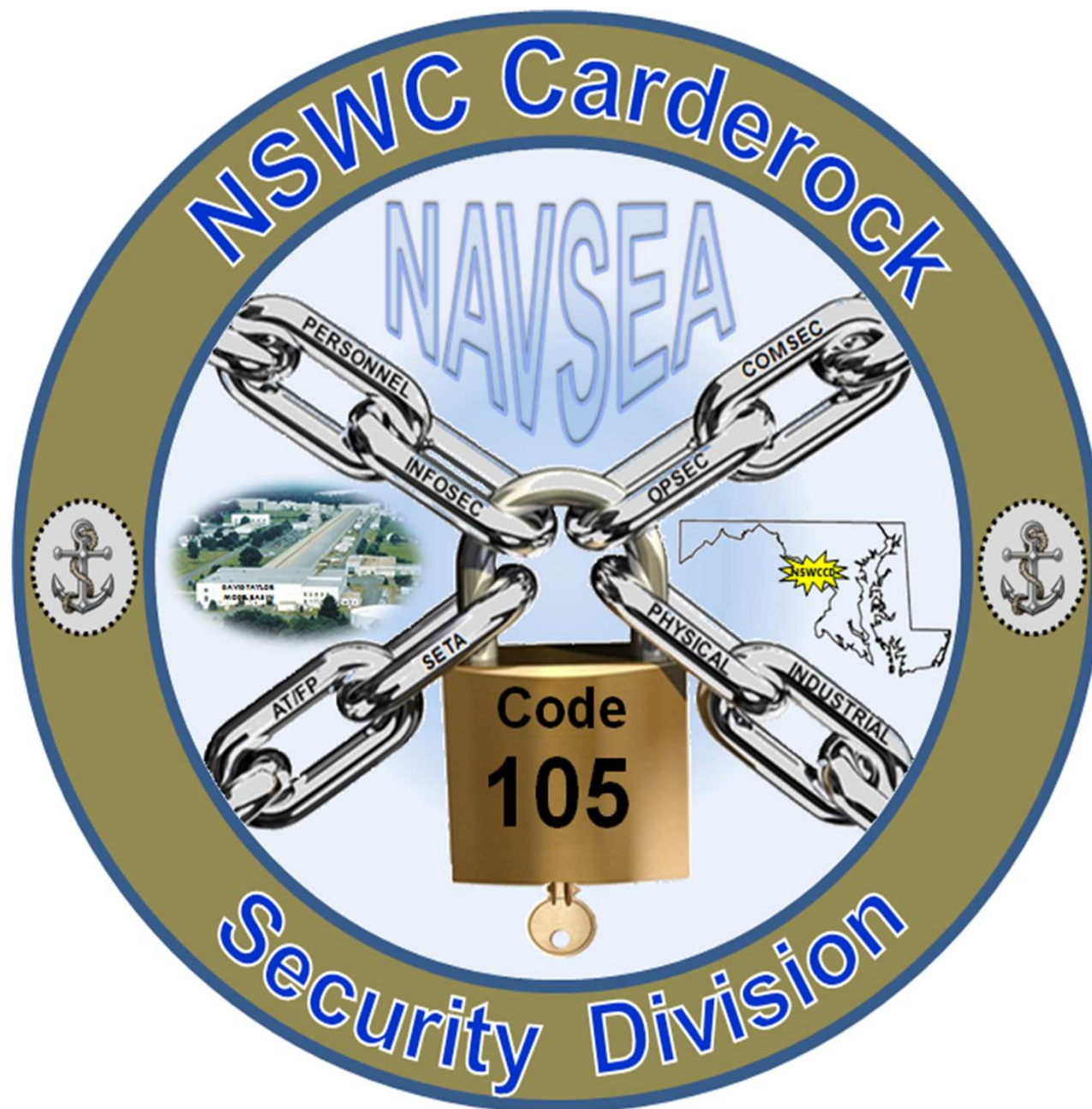
Building 42, Room 104

301-227-1408

vicky.davis@navy.mil

You, Me, Us, We

Security is a TEAM effort!



Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



Controlled Unclassified Information (CUI)

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

*Vicky Davis, Security Policy and
Programs (Code 1051)*

Larry Tarasek
Technical Director, NSWCCD

Controlled Unclassified Information (CUI)

Defined as information that requires safeguarding or dissemination controls pursuant to and consistent with applicable Law, Regulations, and Government-Wide Policies (LRGWP) but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI has its own Executive Order – 13556.

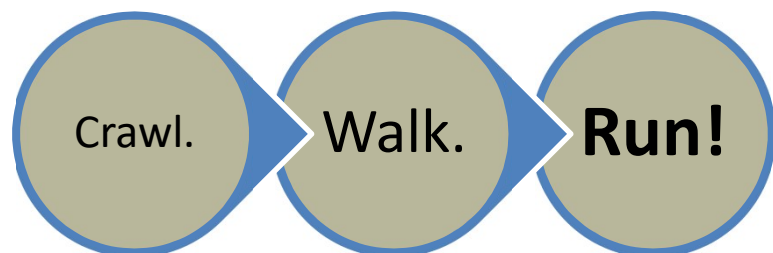
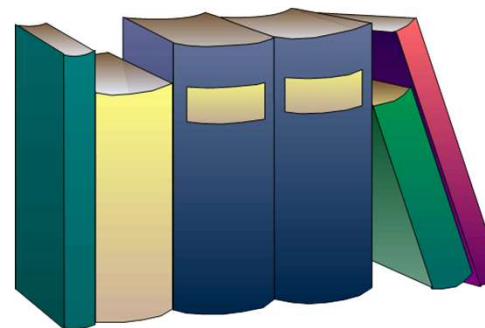


LRGWP

The originator of a document is responsible for determining, at origination, whether the information may qualify for CUI status, and if so, for applying the appropriate CUI markings.

CUI Policy/Resources

- Executive Order 13556
- 32 CFR Part 2002
- DoDI 5200.48
- DoD CUI Registry:
<https://www.dodcui.mil/Home/DoD-CUI-Registry/>
- NSWCCD CUI Desk Guide:
Will soon be published on Cuthill site.
- Training - TWMS #686564 - “DoD Mandatory Controlled Unclassified Information (CUI) Training”



NSWCCD is currently in a “Crawl stage” of a phased NAVSEA implementation plan and not all CUI policy, markings, and training modules are being implemented at this time.

Categories of CUI



Category	Description
Agriculture	Agricultural operation, farming or conservation practices, or the actual land.
Controlled Technical Information*	Information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
Copyright	A form of protection provided by the laws of the United States (17 USC) to the authors of "original works of authorship."
Critical Infrastructure*	The most vital systems and assets (whether physical or virtual), whose incapacity or destruction would have a debilitating impact on the nation's security, economy, and/or public safety.
Emergency Management	Information concerning the continuity of executive branch operations during all-hazards emergencies or other situations that may disrupt normal operations.
Export Control*	Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives.
Financial*	Related to the duties, transactions, or otherwise falling under the purview of financial institutions or United States Government fiscal functions.
Foreign Government Information*	Information provided by, otherwise made available by, or produced in cooperation with, a foreign government or international organization.
Geodetic Product Information	Related to imagery, imagery intelligence, or geospatial information.
Immigration	Related to admission of non-US citizens into the United States and applications for temporary and permanent residency.

Categories of CUI

Category	Description
Information Systems Vulnerability Information	Related to information that if not protected, could result in adverse effects to information systems.
Intelligence	Related to intelligence activities, sources, or methods.
Law Enforcement	Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions.
Legal	Information related to proceedings in judicial or quasi-judicial settings.
North Atlantic Treaty Organization (NATO)	Related to information generated by NATO member countries under the North Atlantic Treaty international agreement, signed on April 4, 1949.
Nuclear*	Related to protection of information concerning nuclear reactors, materials, or security.
Patent	Patent is a property right granted by the Government of the United States of America to an inventor "to exclude others profiting off of or benefiting from the patent owner's property."
Privacy	Personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7).
Proprietary Business Information*	Material and information relating to, or associated with, a company's products, business, or activities; data or statements; trade secrets; product R&D; and performance specifications, etc.
SAFETY Act Information	The regulations implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002.

Freedom of Information Act (FOIA)

- Informs the public of information while appropriately protecting government interests
- Provides individuals with access to many types of records that are exempt from access under the Privacy Act of 1974

**Promotes transparency
& accountability**



Dissemination controls are applied for information that may be withheld from the public if disclosure would reasonably be expected to cause a foreseeable harm to an interest protected under Exemptions 2 through 9 of the FOIA.

FOIA Exemptions

Number	Description
Exemption 2	Information that pertains solely to the internal rules and practices of the agency that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission.
Exemption 3	Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
Exemption 4	Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company.
Exemption 5	Inter- or intra-agency memorandums or letters containing information considered privileged in civil litigation. (Examples: decision making processes and attorney-client privilege.)
Exemption 6	Information, the release of which would reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
Exemption 7	Records or information compiled for law enforcement purposes that: (a) Could reasonably be expected to interfere with law enforcement proceedings. (b) Would deprive a person of a right to a fair trial or impartial adjudication. (c) Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others. (d) Disclose the identity of a confidential source. (e) Disclose investigative techniques and procedures. (f) Could reasonably be expected to endanger the life or physical safety of any individual.
Exemption 8	Certain records of agencies responsible for supervision of financial institutions.
Exemption 9	Geological and geophysical information (including maps) concerning wells.

Why CUI?

- Mixed bag of agency inconsistencies
- Old legacy/ad hoc markings no longer used (not a complete list):



“For Official Use Only” or “FOUO”

“Sensitive But Unclassified” or “SBU”

“Unclassified Controlled Nuclear Information” or “UCNI”

“Law Enforcement Sensitive”, “LES”

“Limited Distribution” or “LIMDIS”

- Legacy markings have been phased out. Mark all new documents and emails containing CUI with “CUI”

- Existing legacy documents do not need to be remarked at this time, as long as they remain under DoD control or are accessed online/downloaded for use within the DoD.



Marking CUI

We are in a NAVSEA “Crawl” phase of a “Crawl, Walk, Run” implementation plan. For now, ONLY:

1. Mark CUI documents/emails with the banner marking of “(CUI)” at the top and bottom of the page/email.
 2. Include a “CUI Designation Indicator” on the bottom right side of the first page/cover of the document, above the CUI footer banner. Example:
 - Controlled by: Department of the Navy (*always this for now*)
 - Controlled by: NSWCCD Code 105 (*agency/office/code making the determination*)
 - CUI Category: OPSEC, PHYS (*from the DoD CUI Registry @ <https://www.dodcui.mil>*)
 - Distribution/Dissemination Control: FEDCON (*Distribution statements B-F or other LDCs*)
 - POC: John Doe, john.doe@navy.mil, 301-555-5555 (*originator/authorized CUI holder*)
- PORTION MARKINGS** →
- Optional in the Crawl phase. If used, they must be applied to all portions, including subjects, titles, paragraphs, bullet points, figures, charts, tables, etc.
 - Required for CUI within classified documents

CUI Marking Examples

MARKINGS ARE FOR TRAINING PURPOSES ONLY

- ✓ Banner markings top/bottom
- ✓ Designation Indicator on right

CUI
(For Training Purposes Only)

MEMORANDUM

From: Head, Policy Management Branch
To: Head, Operations Management Branch
Subj: CUI MARKINGS IN DOCUMENTS

1. This is an example of a document that contains CUI. The CUI banners must be on all pages.
2. CUI portion markings are optional. If used, they must be applied to all portions, including subjects, titles, paragraphs, subparagraphs, bullet points, figures, charts, tables, etc. However, portion markings are required for CUI within classified documents.
3. The CUI Designation Indicator must be on the bottom right of the first page/front cover.

J. D. DOE

Controlled by: Department of the Navy
Controlled by: NSWCCD Code 105
CUI Category: OPSEC, PHYS
Distribution/Dissemination Control: FEDCON
POC: John Doe, john.doe@navy.mil, 301-555-5555

CUI
(For Training Purposes Only)

The screenshot shows an email interface with the following annotations:

- Digitally sign and encrypt:** A red arrow points to the digital signature and encryption icons in the top right corner of the email header.
- Banner Header:** A red arrow points to the text "CUI" at the top of the email body.
- Designation Indicator Box:** A red arrow points to a box containing classification information on the right side of the email body.
- Banner Footer:** A red arrow points to the text "CUI" at the bottom of the email body.

The email content includes a list of instructions for marking CUI emails, such as "This is an example of how to mark CUI emails as of 15 Apr 21. (Attachment contains CUI)" and "All emails containing CUI must be marked with CUI at the top and bottom of the email."

CUI Marking Examples

MARKINGS ARE FOR TRAINING PURPOSES ONLY

	A	B	C	D	E	F	G	H
1			CUI					
2	NAME	ADDRESS	PHONE					
3								
4								
5								
6								

Controlled by: Department of the Navy
Controlled by: NSWCCD, Code 1051
CUI Category: PRVCY
Distribution/Dissemination Control: FEDCON
POC: John Doe, john.doe.civ@us.navy.mil, 301-555-5555

CUI

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE

Brief Date Here
Presenter's Name, Title Here

Brief Title Here

Controlled by: Department of the Navy
Controlled by: NSWCCD Code 60
CUI Categories: CT, PROPIN, SSCL
Limited Dissemination Control: NOCON
Distribution Statement E
POC: Jane Doe, jane.doe1.civ@us.navy.mil, 301-227-1234

CUI

- ✓ Banner markings top/bottom
- ✓ Designation Indicator on right



Distribution Statements on Technical Documents –

“Statements intended to facilitate control, secondary distribution, and release of these documents without the need to repeatedly obtain approval or authorization from the controlling DoD office.”

- A: Approved for public release, distribution is unlimited
- B: Distribution authorized to U.S. Government agencies only
- C: Distribution authorized to U.S. Government agencies/their contractors
- D: Distribution authorized to DoD & U.S. DoD contractors only
- E: Distribution authorized to DoD components only
- F: Further distribution as directed by the Controlling Authority
- X: Use of Distro X is superseded [Convert to Distro C, w/ Export Control]

Distribution Statement “Reasons”

- Public Release
- Administrative or Operational Use
- Contractor Performance Evaluation
- Critical Technology
- Export Controlled
- Foreign Government Information
- Operations Security

TECHNICAL DOCUMENTS

- Premature Dissemination
- Proprietary Information
- Test and Evaluation
- Direct Military Support
- Software Documentation
- Specific Authority
- Vulnerability Information

REFERENCE: DODI 5230.24

Distribution Statements/Controls

Controlled Technical Information (CTI) is a category of CUI

For use on technical documents only (not administrative or general correspondence)

All newly created, revised, or previously unmarked classified and unclassified DoD technical documents must be assigned a distribution statement

Document authors/controlling DoD offices are responsible for initial distribution control determinations/reasons

Wording may not be modified to specify additional distribution

Removal of or tampering with control markings by unauthorized personnel is strictly prohibited

Must remain in effect until changed or removed by the controlling office

Export-controlled data must be marked with applicable export-control statement

YOU are the Subject Matter Expert (SME)!!

Safeguarding CUI

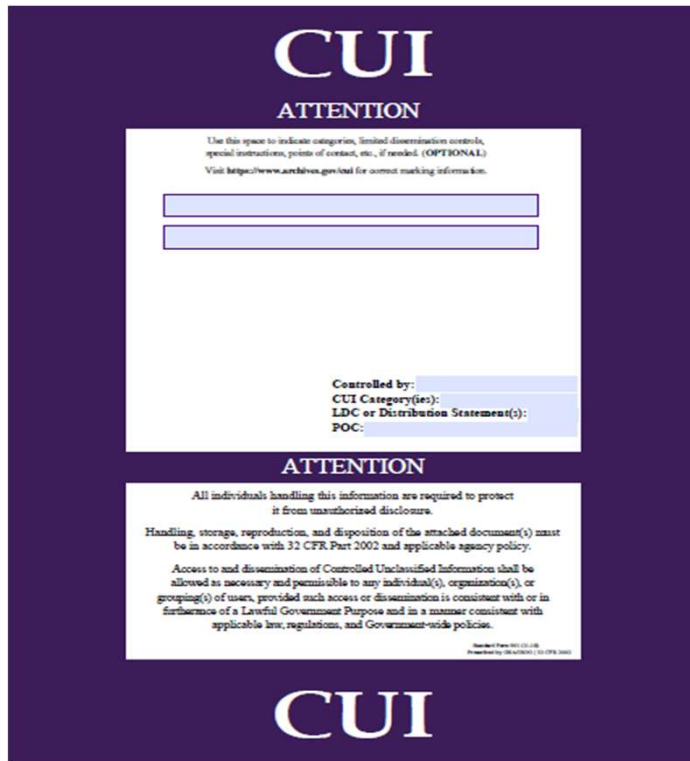


- Be mindful of CUI, viewable/audible, in background/environment when participating on web-based collaboration platforms
- Digitally sign and encrypt all e-mails containing CUI
- Use cover sheets and media labels
- Use First Class Mail; Fax; Parcel Post
- Obtain approval prior to public release



- Discuss CUI on personal devices
- Process or store CUI on personal computers
- Post CUI on public websites or social media platforms

CUI Cover Sheets/Media Labels



CUI
ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc., if needed. (OPTIONAL)
Visit <https://www.archives.gov/ai> for correct marking information.

Controlled by:
CUI Category(ies):
LDC or Distribution Statement(s):
POC:

ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR, Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

CUI

SF 901
Cover Sheet



This medium is
CUI
U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 902 (11-18)

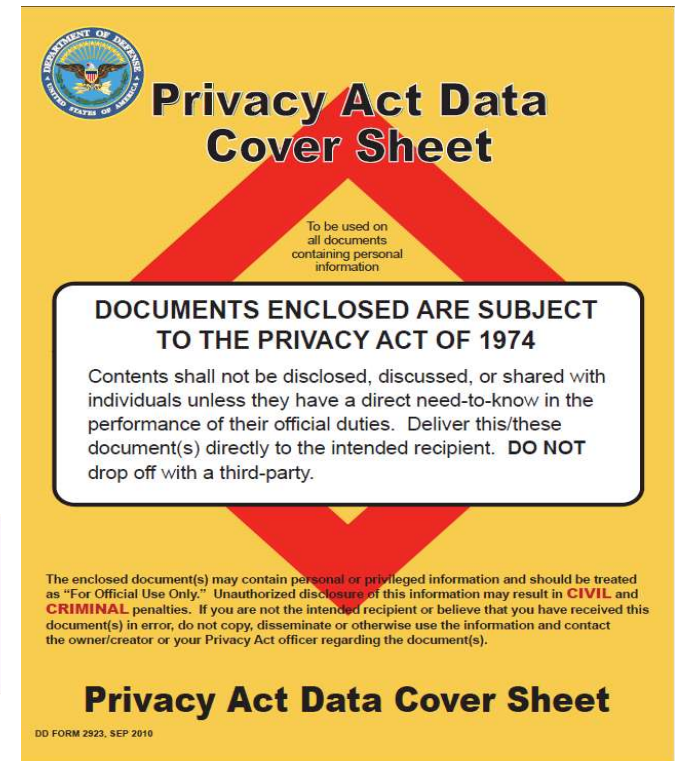
SF 902, CUI
Media Label




This medium is
CUI
U.S. Government Property

SF 903 (11-18)

SF 903, CUI Media
Label: USB size



 **Privacy Act Data
Cover Sheet**

To be used on all documents containing personal information

DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974

Contents shall not be disclosed, discussed, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. **DO NOT** drop off with a third-party.

The enclosed document(s) may contain personal or privileged information and should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in **CIVIL** and **CRIMINAL** penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Act officer regarding the document(s).

Privacy Act Data Cover Sheet

DD FORM 2923, SEP 2010

DD Form 2923
Cover Sheet

Storage of CUI



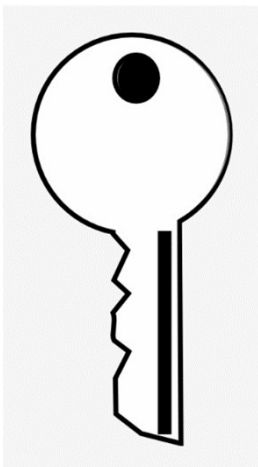
- **During working hours** - minimize the risk of access by unauthorized personnel through eavesdropping or observing CUI on:

- Desks
- Printers/faxes
- Other publicly accessible areas, commute/travel status

- **After working hours** - if space provides security for continuous monitoring (i.e. Open Storage Areas), store in:

- unlocked containers, desks, cabinets, etc.

- For spaces without adequate monitoring, store in locked desks, file cabinets, bookcases, rooms, or similarly secured areas

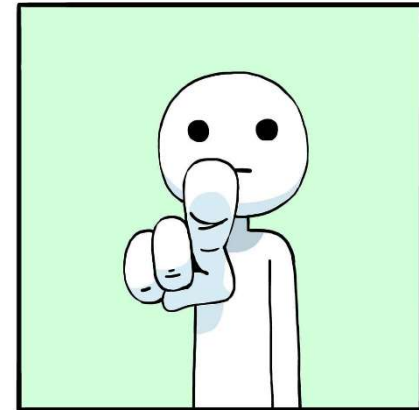


Lawful Government Purpose

- Defined as any activity, mission, function, operation, or endeavor that the Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement)

Similar to the concept of need-to-know for national security classified information

YOU, as the authorized holder of CUI, determine someone's lawful government purpose!



Destruction of CUI

- Any means approved for classified material
- NSA approved cross-cut shredders
- Locked gray shred bins



CUI must be:

- ✓ Unreadable
- ✓ Indecipherable
- ✓ Irrecoverable

- Do not destroy/shred CUI at home. Safeguard and bring back to NSWCCD
- Naval Nuclear Propulsion Information (NNPI) (classified or unclassified) must be destroyed in the same manner as classified information

Our Adversaries Are Relentless



NMCI - “U.S. Says Iran Hacked Navy Computers” – Wall Street Journal (2013)



U.S. Office of Personnel Management (OPM):
21.5 million affected (2015)



“Data Breach at Anthem May Forecast a Trend” – New York Times (2015)



Microsoft: 250 million affected (2019)



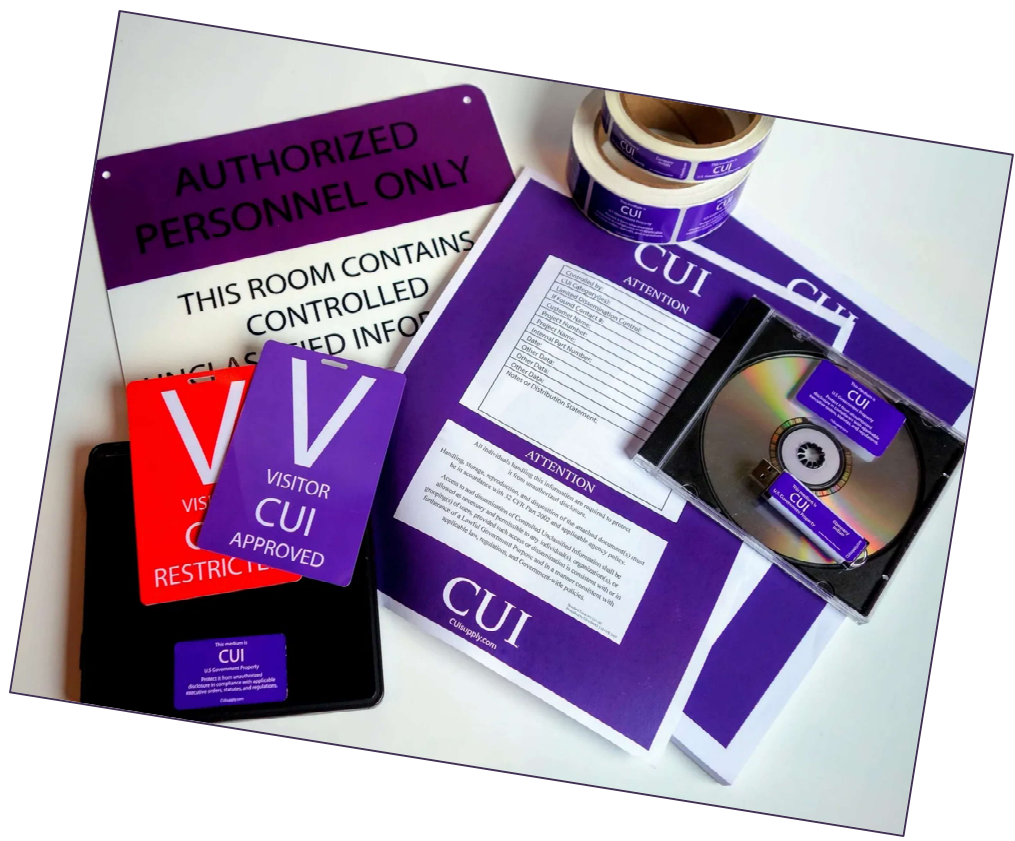
“Twitter Confirms ‘Nation-State’ Attack: User Identities Breached” – Forbes (2020)



Zoom – A breach at the very beginning of the COVID-19 Pandemic (2020)



Questions?



Contact Information



Vicky Davis

Code 105 Security Office

Building 42, Room 104

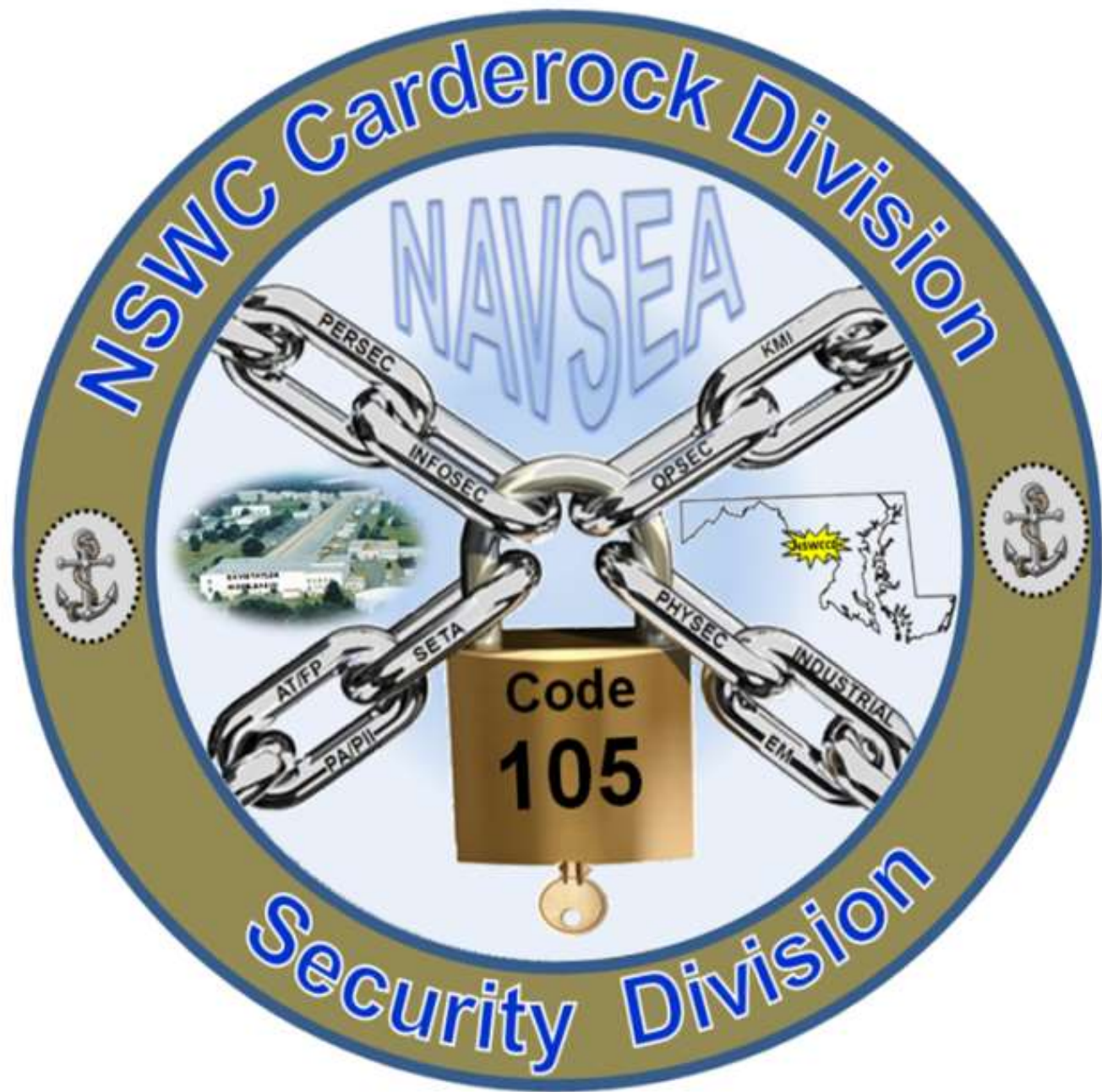
301-227-1408/5410

vicky.l.davis21.civ@us.navy.mil

You, Me, Us, We

*Security is a
TEAM effort!*





Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



Personally Identifiable Information

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

*Vicky Davis, Security Policy and
Programs (Code 1051)*

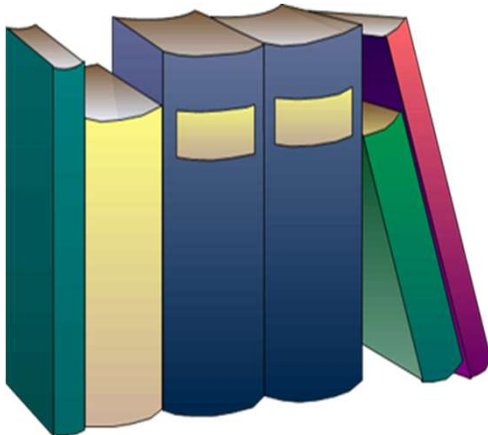
Larry Tarasek
Technical Director, NSWCCD

Personally Identifiable Information (PII)

Defined as information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a SSN; age; rank; grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical and financial information.



PII Policy/Resources



- DoD 5400.11-R, DOD Privacy Program
- SECNAVINST 5211.5F, DON Privacy Program
- NAVSEAINST 5211.2C, NAVSEA Privacy Act – PII Program
- CARDEROCKDIVINST 5211.1B, NSWCCD Privacy Program
- DODI 5200.48, Controlled Unclassified Information (CUI)
- NAVADMIN 125/10, Safeguarding Personally Identifiable Information
- DON MSG DTG 081745Z NOV 12, DON Fax Policy
- DON Chief Information Officer (CIO) website:
<http://www.doncio.navy.mil/Main.aspx>

Helpful Links

- **Encrypting Email Containing PII:**
<http://www.doncio.navy.mil/ContentView.aspx?ID=3989>
- **Rules for Handling PII by DON Contractor Support Personnel:**
<http://www.doncio.navy.mil/ContentView.aspx?ID=2145>
- **PII and Records Management:**
<http://www.doncio.navy.mil/ContentView.aspx?ID=1415>
- **Safeguarding PII on the Command Shared Drive:**
<http://www.doncio.navy.mil/contentview.aspx?id=755>



“Go to” Guidance

Sensitive/Non-Sensitive PII

“High risk” (Sensitive) PII: may cause harm to an individual if lost/compromised:

- Financial information - bank account #, credit card #, bank routing #
- Medical Data - diagnoses, treatment, medical history
- Full or truncated Social Security number
- Place and Date of Birth
- Mother’s maiden name
- Passport #

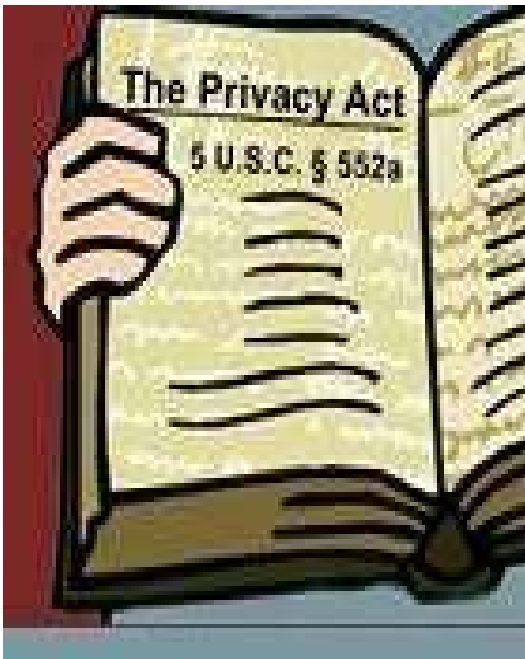


“Low risk” (Non-sensitive) PII: business related PII; releasable under FOIA or authorized use under DON policy:

- Job Title
- Pay grade
- Office phone number
- Office address
- Office email address
- Full Name
- DoD ID/EDIPI
- DoD Benefits number

PII - Information about an individual that identifies, links, relates, or is unique to, or describes the individual which can be used to distinguish or trace an individual's identity.

Privacy Act of 1974



- Privacy Act OF 1974 - governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
- System of Records (SOR) - a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual, such as an SSN.
- No agency shall disclose any record that is contained in a SOR by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

System of Records Notice (SORN)

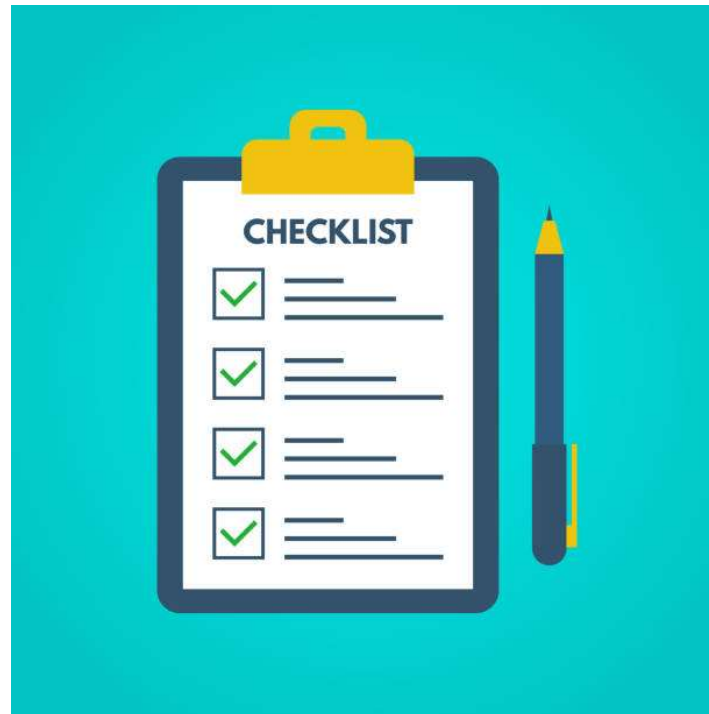


- A public notice of all SOR under DoD control and retrievable by a personal identifier, e.g., name, SSN, date of birth, etc.

- Requirements:
 - Must list authority for soliciting Privacy Act (PA) information
 - Must be published by DoD in Federal Registry
 - Must include a 'Routine Use' Disclosure
 - Must be reviewed annually
 - Can't be deleted, altered or amended
 - Must be posted to Defense Privacy and Civil Liberties Division web site at [http://dpclid.defense.gov/ Privacy/SORNs/](http://dpclid.defense.gov/Privacy/SORNs/)

Your Responsibilities

- ✓ Complete mandatory PII training via TWMS
- ✓ Apply the “lawful government purpose” principle (similar to need-to-know)
- ✓ Do not collect PII without an authorized SORN or maintain an unpublished SOR



- ✓ Obtain a reasonable verification of identity when a request to access PII is made
- ✓ Use DD 2923 and SF 901 Cover Sheets

- ✓ Report violations and/or misuse to your supervisor and PII Coordinator

Controlled Unclassified Information (CUI)



Personally Identifiable Information (PII) is a category of CUI

Apply “lawful government purpose” principle (similar to need-to-know)

Digitally sign and encrypt all emails containing CUI

Properly label and safeguard information

Add CUI banner markings to top/bottom of each page

Add Designation Indicator on right of first page/front cover

Use Cover Sheets:
DD 2923 for PII
SF 901

Store CUI in locked desks, cabinets, etc. when not in use and not already in approved Open Storage Areas

Do not process or store CUI on personal computers/emails or post CUI on public websites/social media platforms

PII/CUI Marking Examples

MARKINGS ARE FOR TRAINING PURPOSES ONLY

- ✓ Banner markings top/bottom
- ✓ Designation Indicator on right

CUI
(For Training Purposes Only)

MEMORANDUM

From: Head, Policy Management Branch
To: Head, Operations Management Branch
Subj: CUI MARKINGS IN DOCUMENTS

- This is an example of a document that contains CUI. The CUI banners must be on all pages.
- CUI portion markings are optional. If used, they must be applied to all portions, including subjects, titles, paragraphs, subparagraphs, bullet points, figures, charts, tables, etc. However, portion markings are required for CUI within classified documents.
- The CUI Designation Indicator must be on the bottom right of the first page/front cover.

J. D. DOE

Controlled by: Department of the Navy
Controlled by: NSWCCD Code 105
CUI Category: OPSEC, PHYS
Distribution/Dissemination Control: FEDCON
POC: John Doe, john.doe@navy.mil, 301-555-5555

CUI
(For Training Purposes Only)

The screenshot shows an email titled "Marking E-mails containing Controlled Unclassified Information - Message (HTML)". The email content includes:

- Header:** "Marking E-mails containing Controlled Unclassified Information" with a "Digitally sign and encrypt" button circled in red.
- Body:** A list of four instructions on how to mark CUI emails, including requirements for banner markings and digital signing/encryption.
- Footer:** Contact information for Vicky Davis, Security Specialist, Code 105, Naval Surface Warfare Center, Carderock Division.

Annotations in red:

- A red arrow points from the "Digitally sign and encrypt" button to a red circle containing a lock icon, labeled "Digitally sign and encrypt".
- A red arrow points from the "Banner Header" text to the "Marking E-mails containing Controlled Unclassified Information" header.
- A red arrow points from the "Banner Footer" text to the "CUI" text at the bottom of the email body.
- A red arrow points from the "Designation Indicator Box" text to the contact information in the footer.

PII/CUI Marking Examples

MARKINGS ARE FOR TRAINING PURPOSES ONLY

	A	B	C	D	E	F	G	H
1			CUI					
2	NAME	ADDRESS	PHONE					
3								
4								
5								
6								

Controlled by: Department of the Navy
 Controlled by: NSWCCD, Code 1051
 CUI Category: PRVCY
 Distribution/Dissemination Control: FEDCON
 POC: John Doe, john.doe.civ@us.navy.mil, 301-555-5555

CUI

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE

Brief Date Here
 Presenter's Name, Title Here

Brief Title Here

Controlled by: Department of the Navy
 Controlled by: NSWCCD Code 60
 CUI Categories: CT, PROPIN, SSCL
 Limited Dissemination Control: NOCON
 Distribution Statement E
 POC: Jane Doe, jane.doe1.civ@us.navy.mil, 301-227-1234

CUI

Distribution Statement Here. Must match above. See slide 3 for guidance.

- ✓ Banner markings top/bottom
- ✓ Designation Indicator on right

Encrypt PII/CUI Emails!!



Digitally sign and
encrypt emails
containing PII/CUI

ALWAYS!!



PII Breach



Breach: Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected.

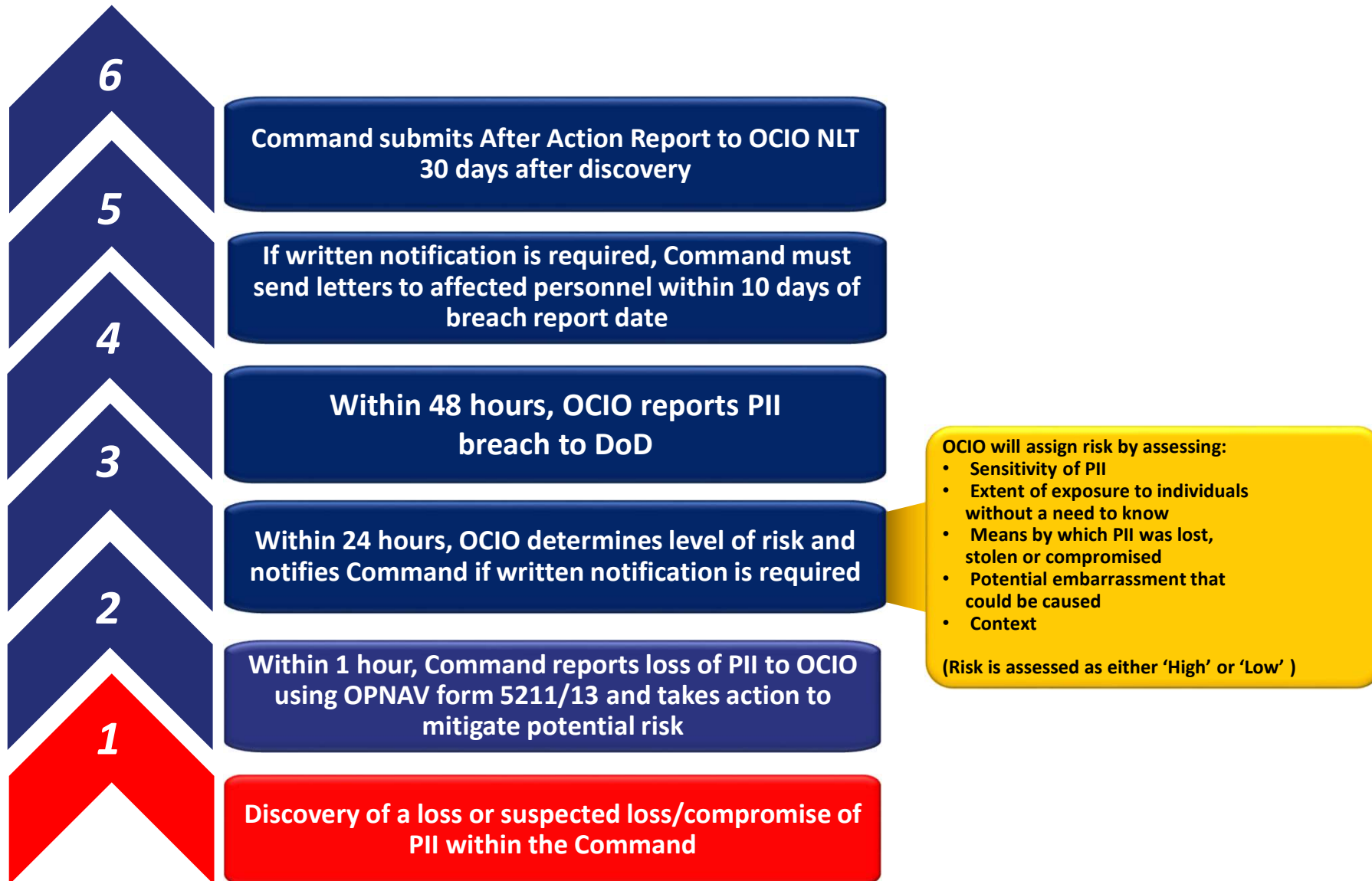
Breach Prevention:

- Complete annual mandatory PII training
- Follow Collections, Maintenance, and Use Policies
- Safeguard/Protect Information
 - ✓ Limit Access
 - ✓ Proper Transmittal (encrypt emails)
 - ✓ Use Coversheets
 - ✓ Proper Disposal
- Report violations and/or misuse to your supervisor and PII Coordinator



DD Form 2923

DON PII Breach Reporting Process



Primary Cause....

- Human error causes 80% of PII breaches
 - Not knowing guidance
 - Failure to follow established guidance
 - Carelessness



The most commonly reported PII breach - failure to encrypt emails
The most commonly breached PII element - SSNs

Faxes and PII



- **Faxing - one of the least secure means to transmit data**

- Uses non-secure phone lines
- Easy to send to wrong person/wrong FAX #
- Copy of transmission often left on machine
- Recipient may not immediately pick up document, exposing PII to others without a lawful government purpose



- **Alternative methods to faxing**

- Send encrypted/digitally signed email
- Use DOD Safe Access File Exchange (SAFE)
- Use United States Postal Service snail mail

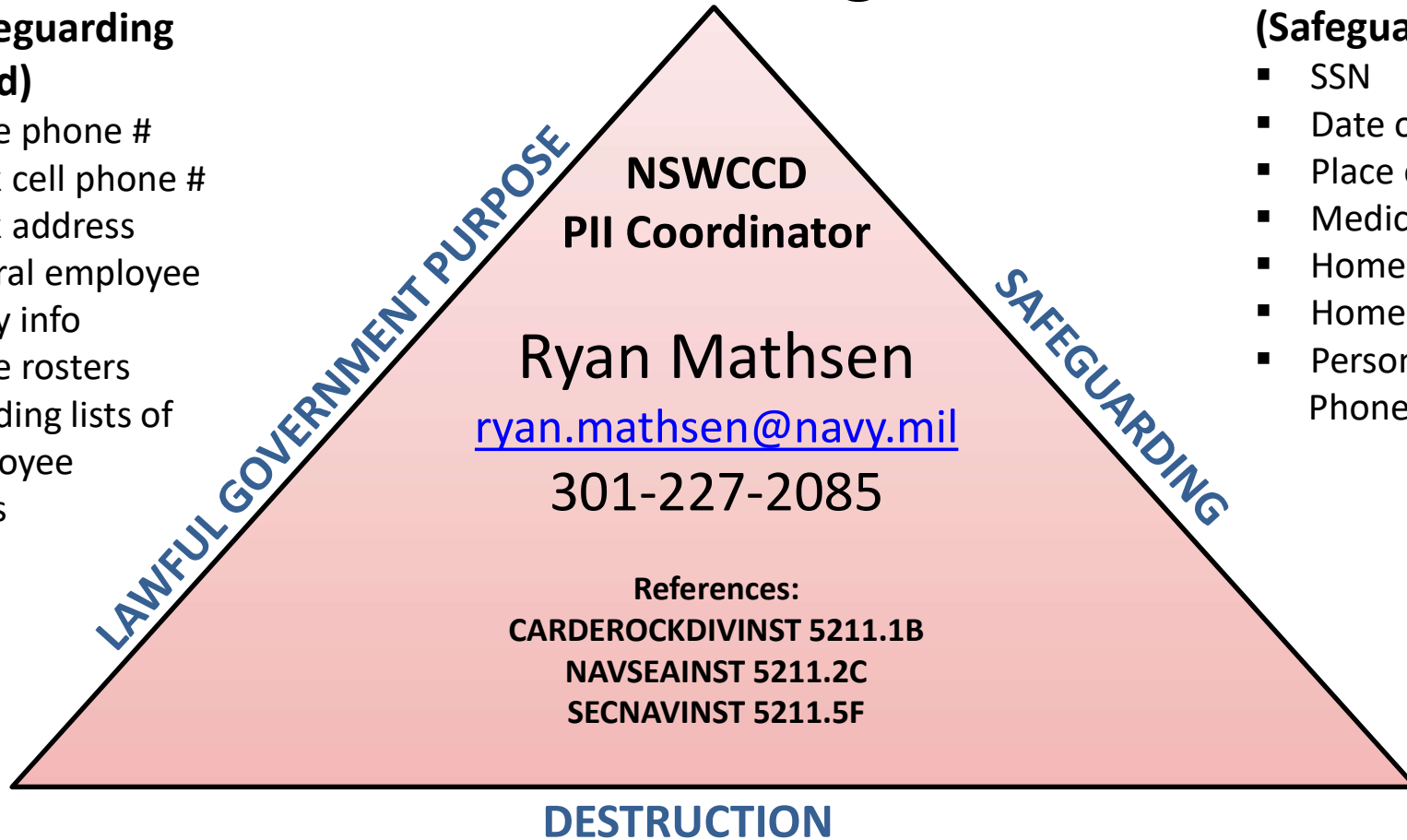
PII Triangle

Non-Sensitive PII (No safeguarding required)

- Office phone #
- Work cell phone #
- Work address
- Federal employee salary info
- Office rosters including lists of employee codes

Sensitive PII (Safeguard)

- SSN
- Date of Birth
- Place of Birth
- Medical Info
- Home Address
- Home Phone #
- Personal Cell Phone #



- **Lawful Government Purpose:** Does the person have a “lawful government purpose” (similar to need-to-know)? If not, do not forward or grant access.
- **Safeguarding:**
 - * Encrypt ALL CUI/PII emails
 - * Use DD 2923/SF 901 cover sheets
 - * Mark CUI on all pages - headers/footers
 - * Add Designation Indicator on first page/cover
- **Destruction:** Only destroy CUI/PII via NSA approved cross-cut shredders or locked gray shred bins. NEVER discard CUI/PII in a trash can, recycle bin, or dumpster.

Questions?



Contact Information



Vicky Davis

Code 105 Security Office

Building 42, Room 104

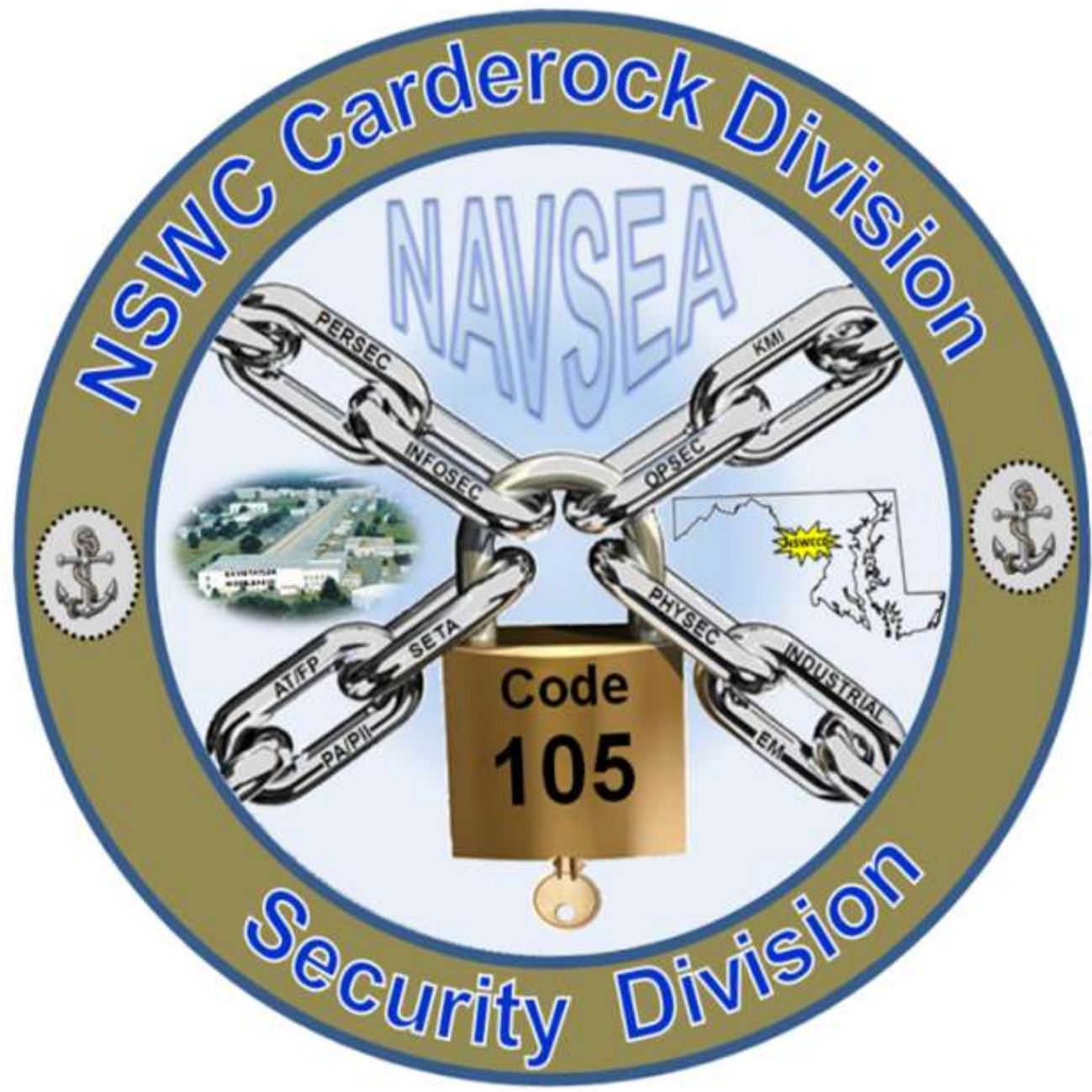
301-227-1408/5410

vicky.l.davis21.civ@us.navy.mil

You, Me, Us, We

***Security is a
TEAM effort!***





Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



Operations Security (OPSEC) Briefing

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

*Robert Gooden, OPSEC Program
Manager*

Larry Tarasek
Technical Director, NSWCCD



Overview

- History
- Definition & Perspective
- Oversight Guidance
- OPSEC & Traditional Security
- Five-Step Process
- OPSEC In-Depth
- OPSEC and the Internet
- TRASHINT
- OPSEC and Public Release
- Miscellaneous



History and Origins of OPSEC

- Developed during the Vietnam War
- Study/analysis of how the enemy gained advance knowledge of combat air operations
- Established a methodology of looking at friendly ops from an adversary prospective
- The effort was code named – Purple Dragon
- Conceived processes to negate/reduce friendly indicators observable by the enemy
- Methodology was termed ‘Operations Security’
- National program formally established in 1988



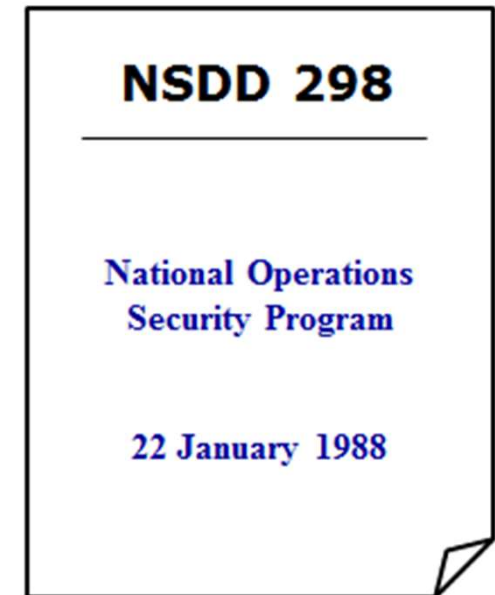
The Purple Dragon

Presidential Authority



- National Security Decision Directive 298, “National Operations Security Program”

Each Executive Department and Agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program ...



-- signed by President Ronald Reagan





OPSEC Defined



A systematic and proven process by which the U.S. Government and its supporting contractors can **deny** to potential adversaries **information** about capabilities and intentions by **identifying**, **controlling**, and **protecting** generally **unclassified** evidence of the planning and execution of sensitive Government activities.

- National Security Decision Directive 298



DoD Directive 5205.02E

- “Applies to all activities that prepare, sustain, or employ U.S. Armed Forces during war, crisis, or peace.”
- “Including activities involving **research, development, test and evaluation; DoD contracting; treaty verification; nonproliferation protocols; international agreements; force protection; and the release of information to the public.**”



SECNAVINST 3070.2

- Establishes policy, procedures, and responsibilities for the Department of the Navy OPSEC program.
- The Secretariat, USN, and USMC shall maintain effective OPSEC programs that ensure coordination between public affairs, cybersecurity, security, operations, acquisition, intelligence, training , and command authorities and include mechanisms for enforcement , accountability, threat awareness, and oversight.
- OPSEC is to be incorporated into all operations and activities.



OPNAVINST 3432.1

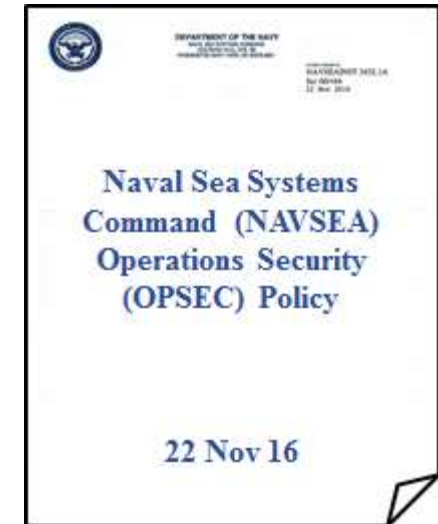
- Directs Echelon II level commands (i.e., NAVSEA), possessing critical information, to establish formal OPSEC programs
- “Essential secrecy will be maintained by naval forces thru use of OPSEC measures..... **OPSEC measures will be applied to research and system development, testing evaluation, and acquisition programs.....**”
- Echelon II level commanders can delegate, to subordinate elements (Carderock), OPSEC program establishment requirements



NAVSEAINST 3432.1A



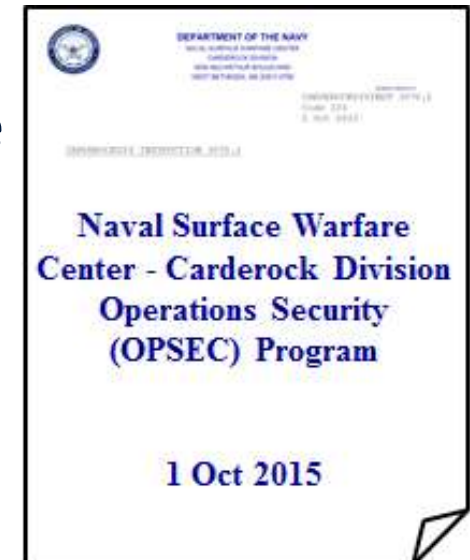
- Directs establishment of OPSEC programs at designated NAVSEA field activities (i.e., Carderock). Delegates responsibility for NAVSEA OPSEC to the Director, Office of Security Programs and Planning
- Applies to all NAVSEA personnel (DoD civilians, military, and on-site contractors)
- “Establish and implement OPSEC policies, procedures, processes and guidance to enable the cost effective protection of NAVSEA critical information, people, technology, essential functions, and equipment.”



CARDEROCKDIVINST 3070.1

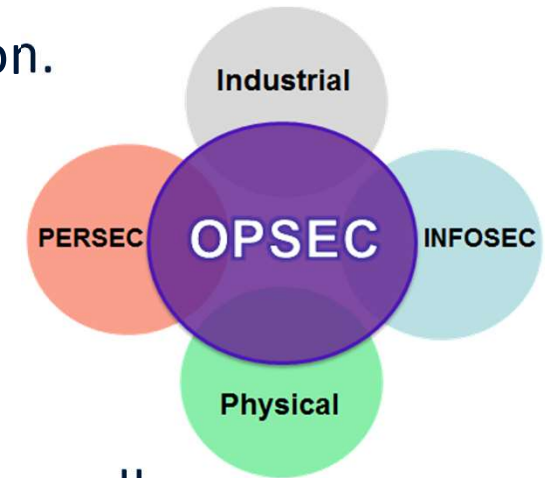


- Directs division commander to establish a Carderock Division OPSEC program and designate a division OPSEC PM (delegated to Security Branch – 105)
- Applies to all departments and offices of Carderock Division
- Supplements OPSEC concepts, policies, and procedures of DON and NAVSEA



Relationship to Traditional Security

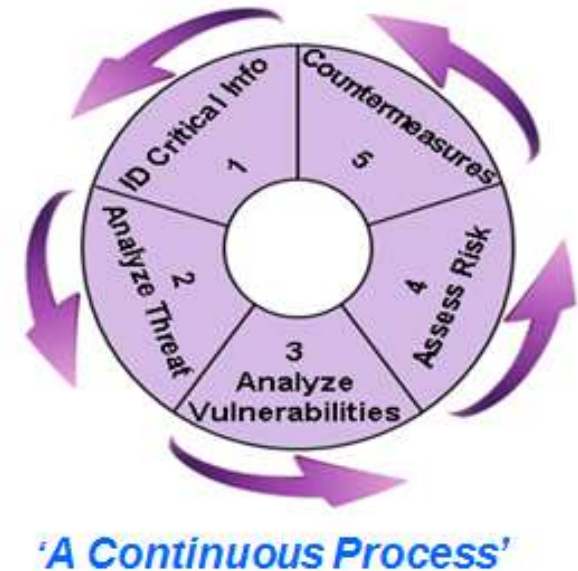
- Security programs protect **CLASSIFIED** information.
 - Personnel Security
 - INFOSEC
 - Industrial Security
 - Physical Security
- OPSEC measures identify, control, and protect generally **UNCLASSIFIED** (critical) information associated with sensitive operations and activities.
- OPSEC is a **COUNTERMEASURES** program.



OPSEC does not replace traditional security disciplines —
it **STRENGTHENS** them.

OPSEC 5-Step Process

- Identify Critical Information
- Analyze the Threat
- Determine Vulnerabilities
- Risk Assessment
- Develop / Apply Countermeasures



OPSEC's most important characteristic is that it is a process that can be applied to any operation or activity.

What is Critical Information?

- Specific facts about friendly intentions, capabilities, and activities
- Probably unclassified, but still sensitive
- Two or three bits of critical information aggregated together may result in a sensitive disclosure



Data aggregation becomes the puzzle pieces revealing the 'big picture'

The information that is often used against us is not classified; it is information that is openly available to anyone who knows where to look and what to ask.

Critical Information



- Command Critical Information List (CIL) and Code specific CIL are posted on intranet
- CO's OPSEC Policy Memo stresses importance of protecting critical information
- Review CIL Cue Cards posted at all desks/workstations

CRITICAL INFORMATION CUE CARD



Critical Information is specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. Because it's normally UNCLASSIFIED, critical information that is an adversary's target of choice.

Seemingly harmless pieces of UNCLASSIFIED information, when combined, can result in an aggregation of sensitive or classified information. Personnel should employ proper Operations Security (OPSEC) procedures to protect critical information.

PROTECT AND SAFEGUARD:

- Controlled Unclassified Information (CUI) such as FOUO, Security Classification Guide (SCG) contents
- Details of plans, programs, operations, test events, exercises, contract awards, designs & milestones before approved for public release
- System/facility vulnerabilities and weaknesses or similar information
- Reference of mission associated information such as personnel/equipment deployment dates/locations
- Privacy Act/Personally Identifiable Information (PII)
- Association of nicknames or code words with programs, projects, or locations

Properly destroy (i.e., shred) hardcopy documents which may reveal CUI or critical information. Encrypt emails that may contain or reveal CUI or critical information.

Implementing OPSEC at work and home enables mission success by reducing adversary options to collect critical information or personal information. Become a hard target! For more information contact the NSWCCD Security Division at 301-227-1861/1408.

March 2017



Analyze the Threat

“The capability of an adversary coupled with the intention to undertake any actions detrimental to the success of program activities or operations.”

- Nation states
- Insiders
- Criminal elements
- Terrorists
- Narcotics traffickers

<i>Threat Actors</i>	<i>Motive</i>	<i>Targets</i>	<i>Means</i>	<i>Resources</i>
<i>Nation States During War Time</i>	Political	Military, intelligence, infrastructure, espionage, reconnaissance, influence operations, world orders	Intelligence, military, broad private sector	Fully mobilized, multi-spectrum
<i>Nation States During Peace Time</i>	Political	Espionage, reconnaissance, influence operations, world orders	Intelligence, military, leverages criminal enterprises or black markets	High, multi-spectrum, variable skill sets below major cyber powers
<i>Terrorists, Insurgents</i>	Political	Infrastructure, extortion	Leverage black markets?	Limited, low expertise
<i>Political Activists or Parties</i>	Political	Political outcomes	Outsourcing?	Limited, low expertise
<i>Black Markets For Cyber Crime</i>	Financial	Hijacked resources, fraud, theft, IP theft, illicit content, scams, crime for hire	Tools, exploits, platforms, data, expertise, planning	Mobilizes cyber crime networks
<i>Criminal Enterprises</i>	Financial		Reconnaissance, planning, diverse expertise	Professional, low end multi-spectrum, leverage of black markets
<i>Small Scale Criminals</i>	Financial		Leverages black markets	Low, mostly reliant on black markets
<i>Rogue Enterprises</i>	Financial	IP theft, influence on sectoral issues	Outsourcing to criminal enterprises?	Sectorial expertise, funding, organization

Threat Actors and Capabilities

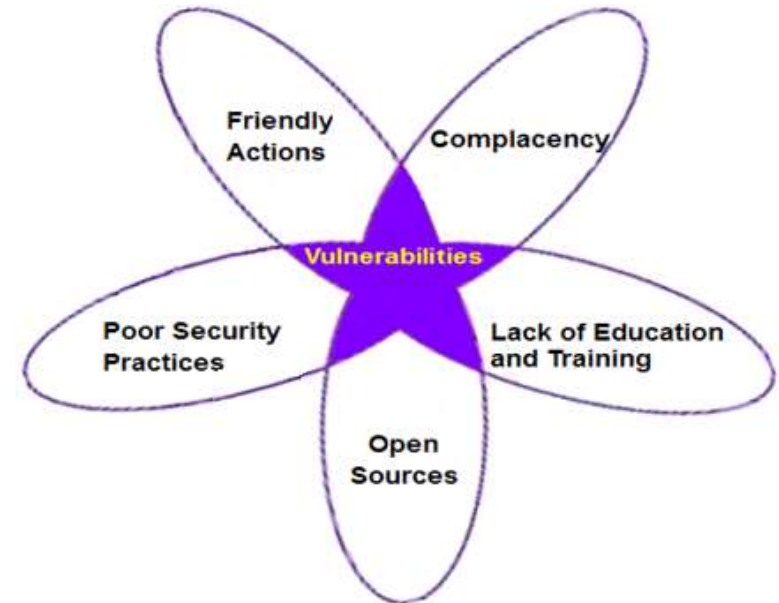
Threat = Capability + Intent



Vulnerabilities

‘Weaknesses which are susceptible to exploitation by adversaries. A vulnerability exists when the adversary is capable of collecting an OPSEC indicator, correctly analyzing it, and then taking timely action.’

- Observation of friendly actions
- Open source research
- Poor security processes
- Lack of education and training
- Complacency / predictability



Vulnerability + Threat = Risk

Indicators

‘Friendly actions and open sources of information that can be detected or interpreted by adversarial intelligence systems.’

- Signatures – make indicators identifiable and stand out
- Associations – relationships to other information or activities
- Profiles - sum of multiple signatures (patterns)
- Contrasts - established pattern vs. current observations
- Exposure – duration and time an indicator can be observed

Allows the adversary to identify our critical information

Risk Assessment

- Risk management, not risk avoidance
- **Threat** + No Vulnerability = No Risk
- No Threat + **Vulnerability** = No Risk
- ***Threat + Vulnerability = Risk***
- Justify the cost of losing information vs. the cost of implementing countermeasures

Risk is the likelihood of an undesirable event occurring and the consequences of that event.



Apply Countermeasures

- Prevent detection of critical information
- Provide an alternative association of critical information
- Deny the adversary's collection system
- Implement new, more stringent procedural actions

\$\$\$ - Cost is the biggest factor in implementing specific countermeasures

Basic Countermeasures

- All Paper, Notes, Printouts etc.– **NAVSEA Shred Policy**
- Sensitive/classified e-mails – **Encryption or use SIPRNET**
- Phone Calls – **STE**
- Sensitive/classified info documents – **SIPR/Secure Fax**
- DO NOT **“TALK AROUND”** Sensitive Information on Non-Secure Voice Circuits
- No **“Pillow Talk”** (guard what’s shared with significant others)
- No **“Shop Talk”** in restaurants, bars, public areas

The best countermeasure is to adhere to established security procedures

OPSEC and the Internet



- Recovered al Qaida training manual states:
 - “Using public sources openly and without resorting to illegal means, it is possible to gather at least **80%** of information about the enemy”
- DoD Website Admin Policy - review data for sensitivity before posting to publicly accessible websites (www.defenselink.mil/webmasters)
- OPSEC policy requirement to conduct periodic web site reviews/research for presence of sensitive information

Policy requirement for OPSEC PMs to conduct periodic web site reviews/research for presence of sensitive information



Social Networking Sites

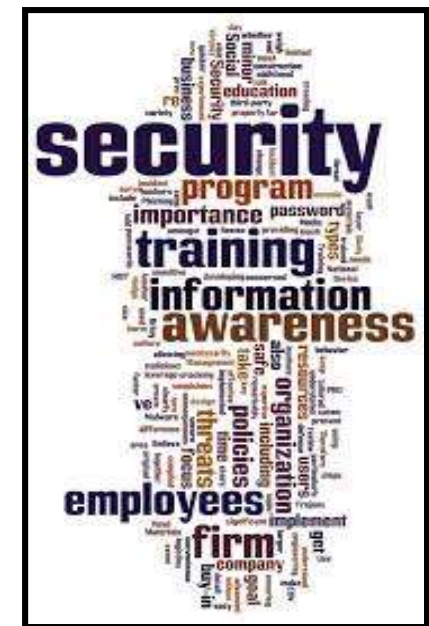
- Current problem
- Adhere to SECDEF DoD policy
- Jun 2009 Deputy Director Memo
- Absolutely no expectation of privacy
- Pose a **significant** OPSEC, intelligence, and general security **threat to DON personnel, facilities, and mission**

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a dark blue rectangular background.The Twitter logo, consisting of the word "twitter" in a light blue, lowercase, sans-serif font with a thin blue outline, set against a white background with a dashed border.

DON employees are prohibited from posting information about DON personnel, missions, activities, and operations unless it is readily available to the general public AND has been authorized of public release IAW DoD guidance

OPSEC and Official IT Networks

- Technical nature of system passwords warrant added protections
- Don't share passwords with co-workers or unauthorized users
- Risks are information compromise/system degradation
- Sys Admins: Transmit router settings and passwords separately and always encrypt



CTF 1010 MSG, DTG 120537Z AUG 17, Subj: OPSEC Handling of Network Settings and Passwords



Our Adversaries Are Relentless



“Australian defense firm was hacked and F-35 data stolen, DoD confirms” – arstechnica.com, 2017



The Washington Post
Democracy Dies in Darkness

National Security

China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare



2018

THE WARZONE

What Secretive Anti-Ship Missile Did China Hack From The U.S. Navy?

Details surrounding the Navy's Sea Dragon program remain scarce, but there are some distinct possibilities.

BY TYLER ROGOWAY AND JOSEPH TREVITHICK JUNE 8, 2018

- THE WAR ZONE
- ANTI-SHIP MISSILE
- CYBER WARFARE
- ESPIONAGE
- HACK
- HACKED
- HYPERSONIC
- LRASM
- LRASM-B
- NETWORKED
- NUWC RHODE ISLAND
- RATTLRS
- SEA DRAGON
- SM-6
- STRATEGIC CAPABILITIES OFFICE
- SUBMARINE
- TIME-SENSITIVE STRIKE

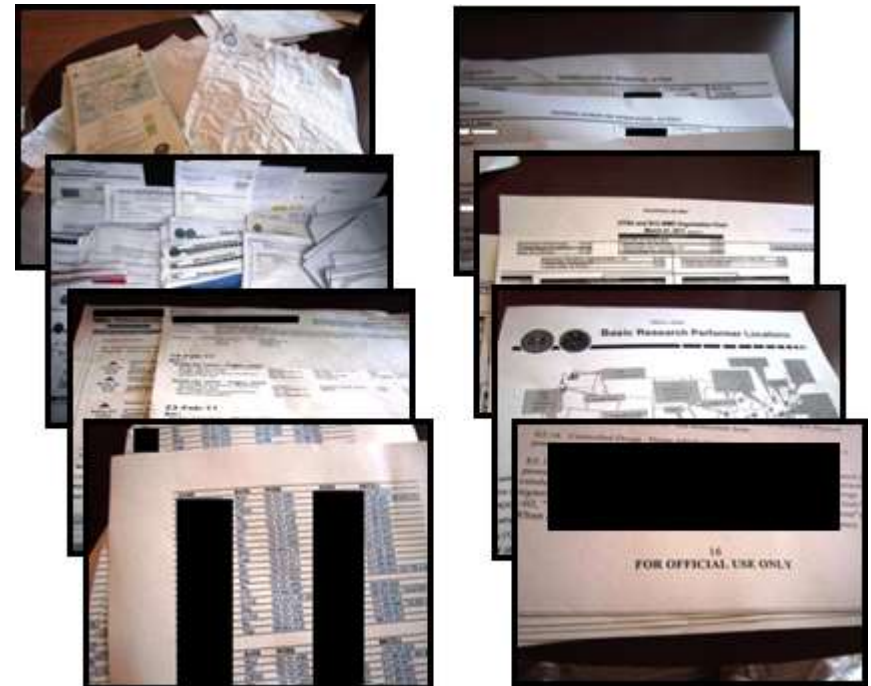


TRASHINT

Dumpster-dives of random refuse collection points

Examples of Critical Information Found

- Personally Identifiable Info (PII)
- Official e-mails
- Funding/resource/budget information
- Office Memos
- FOUO
- Personal banking account numbers
- Technical briefings





TRASHINT Countermeasures



- Periodically inspect outgoing trash and recycle containers
- Utilize approved shredders and burn bags
- Securely store sensitive information pending destruction





OPSEC and Public Release



- Official news articles
- Briefing presentations
- Training/informational brochures, pamphlets, etc.
- Manuscripts for books/movies/plays (fiction or non-fiction)
- Personal (unofficial) blogs
- SNS forums
- Ensure applicable time allowance (edits/conflicts)
- Restrictive/Limited Distribution Statements (A-F)

Pre-publication review is mandatory IAW DoDI 5230.29; DEPSECDEF & CJCS Jnt Msg DTG 090426Z AUG 06; DoDI 8550.01; and DoD 5205.02-M. Additionally, SF-312, Nondisclosure Agreement.



OPSEC: Capture The Flag

|

OPSEC: Capture The Flag



Your Responsibilities

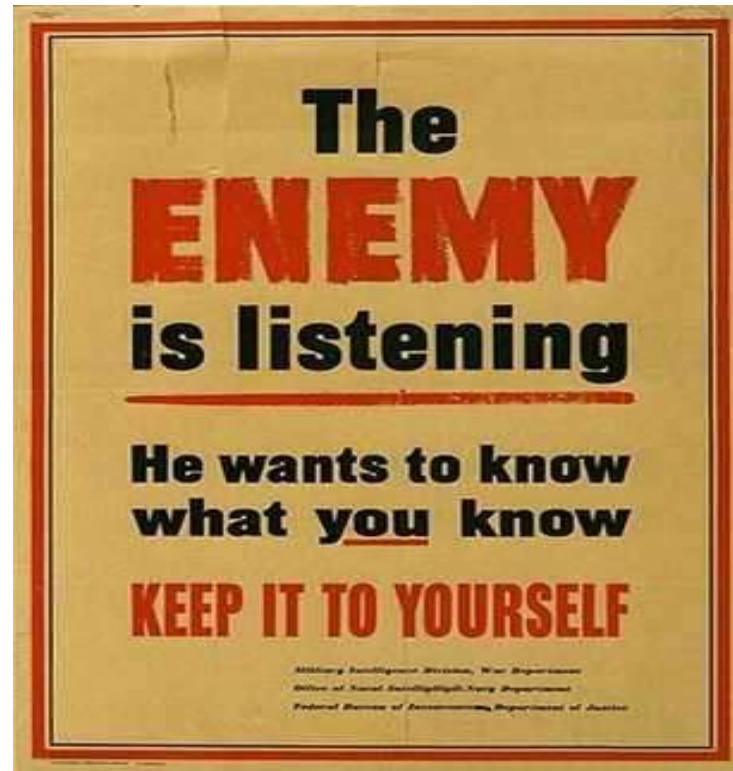
- Ask Yourself --
 - ✓ Is this information important to our adversaries?
 - ✓ Do I care if it is **published on the front page** of the Washington Post?
 - ✓ Will it help an adversary to assemble and form the **overall picture**?
 - ✓ Is this information central to the mission effectiveness of NSWCCD or my office?
 - ✓ What might this “insignificant” information reveal to adversaries about our **intentions** and **capabilities**?
- What will our adversaries learn by watching, listening, and collecting information we “protect?”

OPSEC Summary

- **Identify critical information** to determine if friendly actions can be observed by adversary intelligence systems.
- **Determine if information** obtained by adversaries **could be interpreted** to be useful to them.
- **Execute** selected **countermeasures** that eliminate or reduce adversary exploitation of friendly critical information.

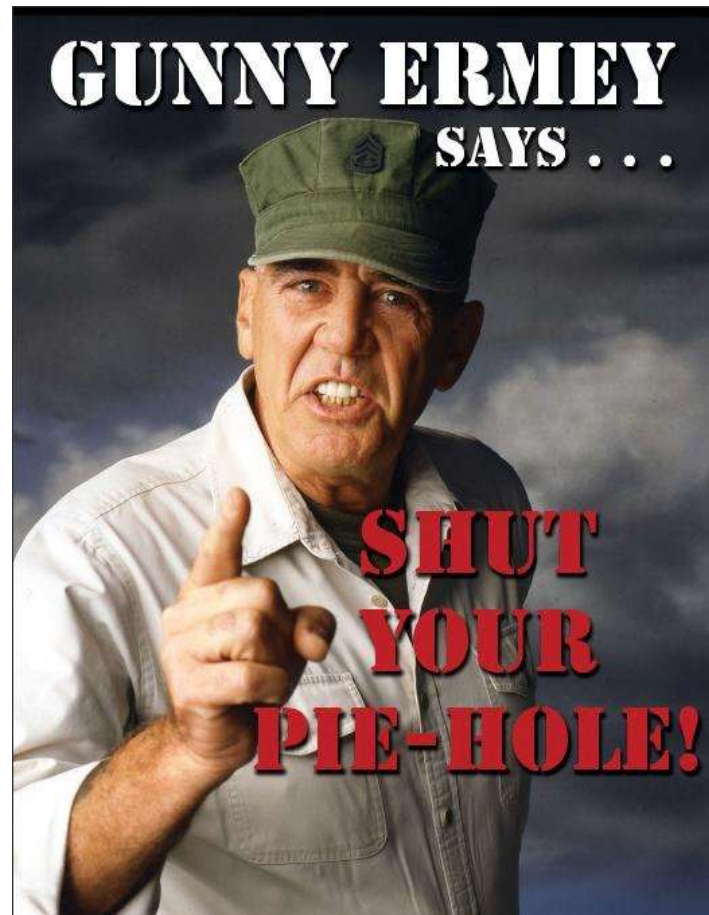
OPSEC helps identify the indicators that give away information about missions, activities and operations.

Still Important Today



World War II Era Poster

Still Important Today



Modern Era Poster

Contact Information

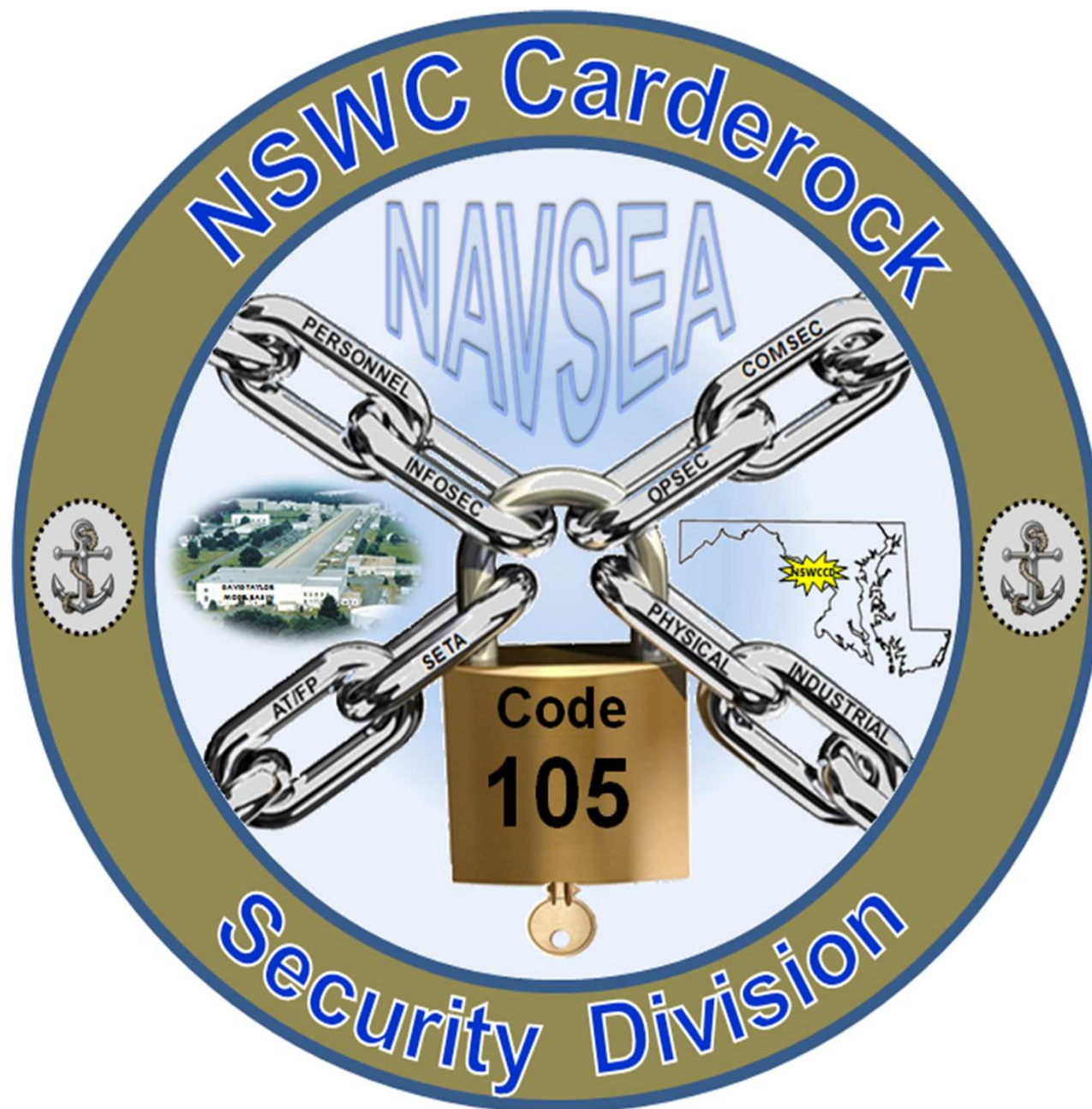


Cliff Young
Security Division (Code 105)
Building 42, Room 104
301-227-1861
Clifford.young@navy.mil

Remember...Think OPSEC!!

**Security is Everyone's Responsibility – If You See
Something, Say Something!**





Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



DoD Level-1 Antiterrorism (AT) Training for New Hires

Homer Renshaw

Captain Todd E. Hutchison

Commanding Officer, NSWCCD

1052 (Security Division)

Larry Tarasek

Technical Director, NSWCCD



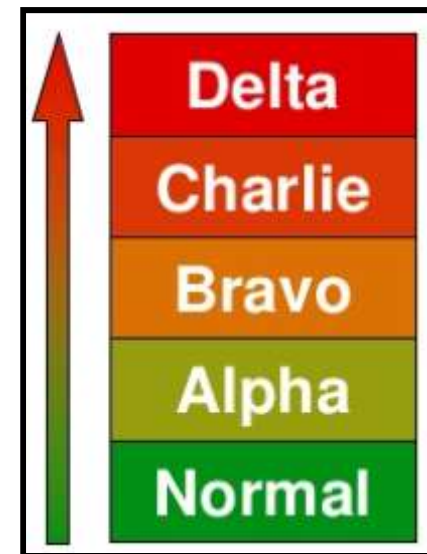
Introduction

- Threat is a real and present danger
- Remain vigilant while executing responsibilities
- International terrorist network may be present where you serve
- Personal safety is important
 - Remain alert
 - Be aware of your surroundings
 - Report suspicious activity
 - Pay attention to antiterrorism briefings
 - Make security part of your routine
- Do not be a tempting target!

America's effort to fight terrorism includes everyone.

Force Protection Conditions

- US military facilities use protective measures organized in a system called Force Protection Conditions, or FPCONs.
- FPCONs are organized in five levels with increased protection at each level:
 - NORMAL
 - ALPHA
 - BRAVO
 - CHARLIE
 - DELTA.



As the threat of attack changes, Commanders change the FPCON to protect personnel

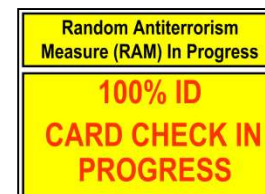
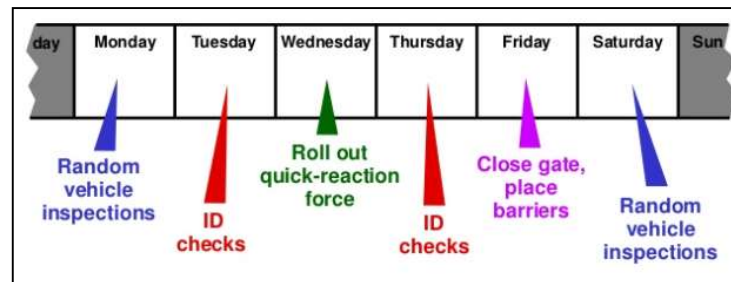


FPCONs (cont.)

- **NORMAL** – Routine security posture (access controls)
- **ALPHA** – Increased threat (maintain indefinitely)
- **BRAVO** – Increased/predictable threat (operational effects)
- **CHARLIE** – Per intel, event likely (prolonged hardships)
- **DELTA** – Actual/imminent event (not for extended duration)

Random Antiterrorism Measures (RAM)

- Supplement FPCONs
- Countermeasure to hostile force observation
- HHQ approval
- Provides change to security atmosphere



Anticipate

- Anticipating threats, risks, and vulnerabilities is fundamental to antiterrorism and personal security.
- Ways to do this include:
 - Research criminal activity
 - Understand the tactics & techniques
 - Know types of targets and locations
- Consider consulting these sources
 - Police crime reports
 - Other internet and media resources



Several sources allow you to research threats for yourself

Be Vigilant

- Vigilance is required to continuously observe your surroundings and recognize suspicious activities.
- Understand your environment's normal conditions.
- Knowledge of the normal amplifies abnormal activities.
 - Items that are out of place
 - Attempted surveillance
 - Circumstances that correspond to prior criminal activity in your area



Informed vigilance is fundamental to personal security

Don't Be a Target

- Blend in with your surroundings.
 - Do not wear clothing or carry items that attract criminal attention
 - Remain low key
 - Avoid high criminal locations
- Reduce your vulnerability and exposure:
 - Select places with security measures
 - Be unpredictable
 - Travel in a small group
 - Use automobiles and residences with adequate security features



DOD affiliation may identify you as a potential target

Report and Respond

- Report suspicious activities to appropriate authorities.
 - Report suspicious activity, do not try to deal with it yourself
 - In threatening situations, take steps to reduce your exposure
 - Follow the instructions of emergency personnel and first responders



(The Fort Dix attack plot was thwarted by an alert store clerk)

Security is a team effort

Active Shooter Intro

- An Active Shooter incident can occur any time, any place
 - September 2013 shooting at the Navy Yard
 - March 2011 shooting of Air Force personnel at Frankfurt Airport in Germany
 - November 2009 shooting at the Soldier Readiness Center in Fort Hood, Texas
 - June 2009 shooting at the Holocaust Museum in Washington, D.C.
 - May 2009 shooting of soldiers outside a military recruitment center in Arkansas
 - 2007 plot to attack Fort Dix using automatic weapons
- Active Shooter incidents are unlikely, but you should be prepared for the possibility.



An incident can occur anywhere, even on your own installation

Active Shooter Fundamentals

- Responses to an Active Shooter include:
 - Run
 - If you can escape the area, do so without hesitation
 - Hide
 - If unable to escape, find a place to hide
 - Fight
 - As a last resort, and only if your life is in immediate danger, alone, or as a group, attempt to incapacitate the shooter.



Run, Hide, Fight

Responding to an Active Shooter

- Evacuate: If possible, be sure to:
 - If you can escape, do so without hesitation. Be aware that your evacuation point may be different than for fire evacuations.
 - Evacuate whether others agree to or not.
 - Leave your belongings behind.
 - Help others escape, if possible. Assist individuals with special needs or disabilities.
 - Attempt to rescue others or treat the injured only if you can do so without further endangering yourself or others.
 - Keep your hands visible as you flee.
 - Prevent others from entering the area, if possible.



Run

Responding to an Active Shooter 2

- If unable to escape, find a place to hide.
- Your hiding place should:
 - Be out of the shooter's view.
 - Provide protection from shots fired (e.g., hide behind large items that afford protection).
 - Prevent shooter from entering (e.g., barricade the door with furniture).
- Silence cell phones/turn off any source of noise (e.g., radios).
- Remain quiet.
- Identify improvised weapons.
- Attempt to rescue others or treat injured only if you can do so without further endangering persons inside a secured area



Hide

Responding to an Active Shooter 3

- As a last resort, and only if your life is at immediate risk, together or alone, attempt to incapacitate the shooter.
 - Act as aggressively as possible against the shooter.
 - Throw items and improvised weapons.
 - Yell.
- Be committed to your actions until the shooter is eliminated.



Fight

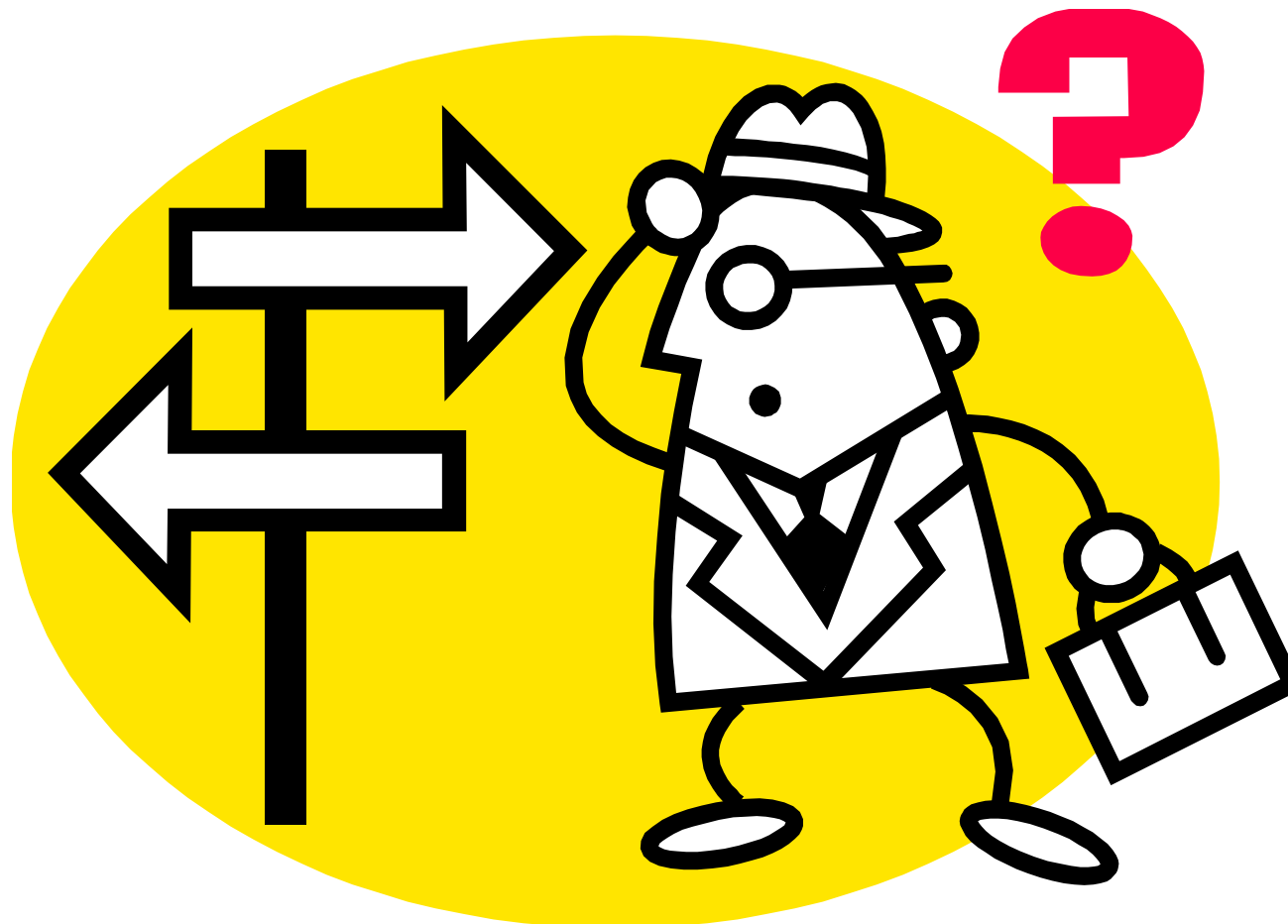
Arrival of First Responders

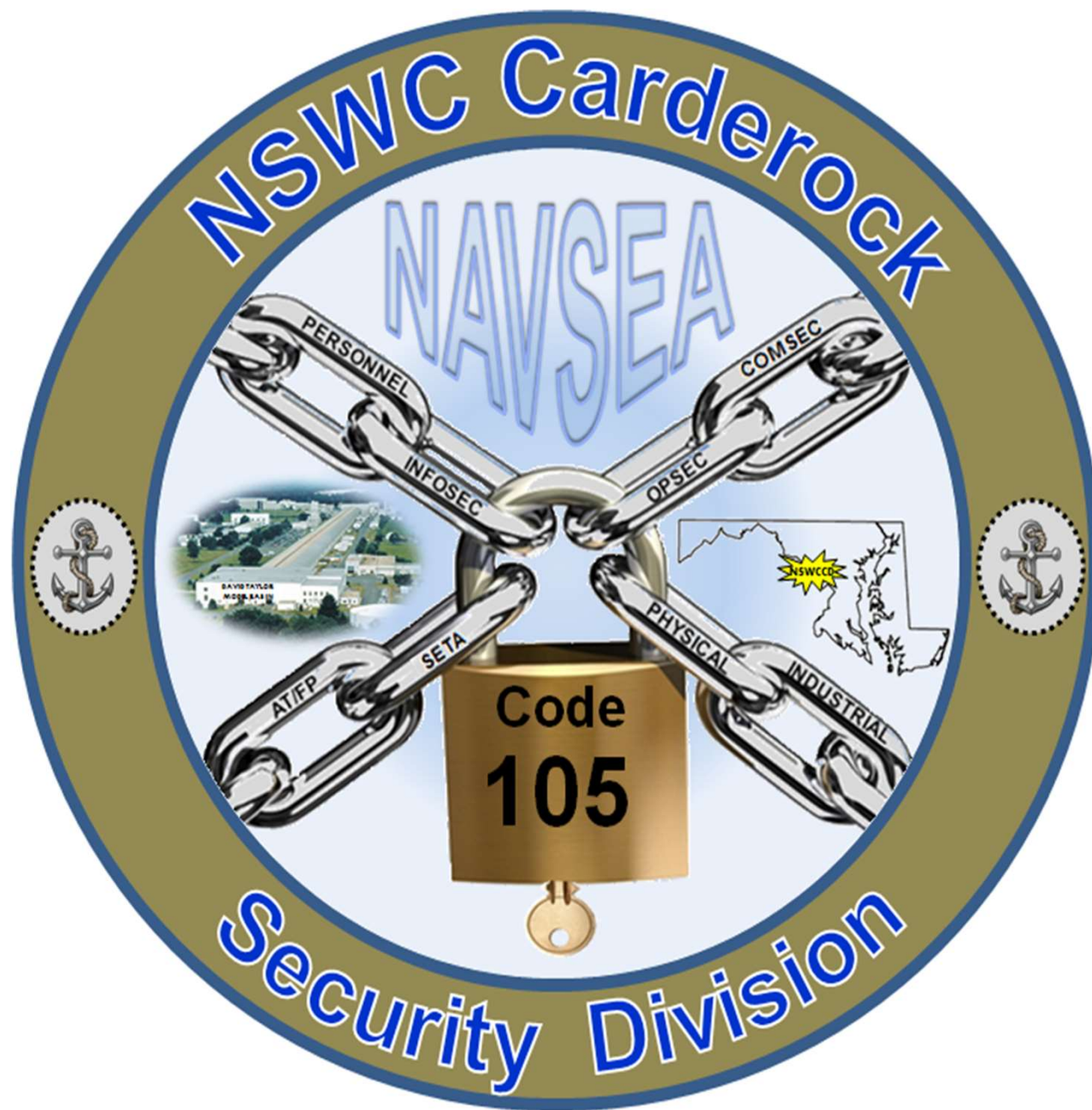
- When first responders arrive, support their efforts and do not be a distraction:
 - Officers will move directly to where last shots were heard.
 - Remain as calm as possible and follow Officer's instructions. You may be searched.
 - Avoid quick movements, do not point.
 - Put down items in your hands; raise hands and keep hands visible at all times.
 - Officers may shout commands and push individuals to the ground for their safety.
 - Do not attempt to hold onto Officers for safety.
 - Do not stop to ask Officers for help - proceed in the direction they have approached from.
 - Remember, LE's mission upon arrival is to stop the shooter, rendering aid is secondary.



Cooperate with first responders and don't be a distraction

Questions





Lunch

See you back at 12:30!



Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



FY22 Insider Threat Awareness Training

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Security Division (Code 105)

Larry Tarasek
Technical Director, NSWCCD

Insider Threat POCs



**Rachael Bass (Program
Manager)**
rachael.t.bass.civ@us.navy.mil

Terry Tate (Alternate)
terry.l.tate.civ@us.navy.mil

Brandon Reilly (Branch Chief)
brandon.r.reilly.civ@us.navy.mil

For general security information and inquiries call: 301-227-1408

Insert appropriate Distribution or CUI statement here

Insider Threat Agenda



- **Security Message**
- **Basic Insider Threat Definitions**
- **Significance of Insider Threat**
- **Fighting the Insider Threat**
- **Recognizing the Insider Threat**
- **Reporting the Insider Threat**
- **Case Studies**
- **Summary**

Insert appropriate Distribution or CUI statement here

Security Message

The protection of U.S. Government assets including people, property, and both classified and controlled unclassified information is the responsibility of each and every member of the Department of Navy (DON), regardless of how it was obtained or what form it takes. Anyone with access to these resources has an obligation to protect it; a simply “I didn’t know” just won’t cut it.

The very nature of our jobs dictates we must lead the way in sound security practices. This Insider Threat training provides an overview for security education, training, and awareness.

Our vigilance is imperative!

Basic Insider Threat Definitions

Insider threat - a person with authorized access, who uses that access wittingly or unwittingly to harm national security interests through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss of degradation of resources or capabilities. The term kinetic can include, but is not limited to, “the threat of harm from sabotage or workplace violence.”

Insider - Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD.

Threat - A person having the intent, capability, and opportunity to cause loss or damage.

Access -The ability and opportunity to obtain knowledge of classified sensitive information or to be in a place where one could expect to gain such knowledge.

Asset - Person, structure, facility, information, material, or process that has value.

Classified Information - Official information that has been determined to require, in the interests of national security, protection against unauthorized.

Basic Insider Threat Definitions (continued)



Cleared Contractor (CC) - A person or facility operating under the National Industrial Security Program (NISP) that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level.

Controlled Unclassified Information - Unclassified information that does not meet the standards for National Security Classification under EO 12958 but is (1) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

Disgruntled Employee - An employee who may be annoyed, discontent, displeased, dissatisfied, grumpy, irritated, malcontent, or upset to the point that he may take violent action against a coworker, supervisor, or employer.

Personal Identifiable Information (PII) - Information that can be used to distinguish or trace an individual's identity. This includes: names; social security number; date and place of birth; rank/paygrade, phone number and biometric records or any other personal information that is linked or linkable to a specified individual.

Risk - a measure of consequence of peril, hazard, or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).

Insert appropriate Distribution or CUI statement here

Why is the Insider Threat Significant

An insider threat can have a negative impact on national security and industry resulting in:



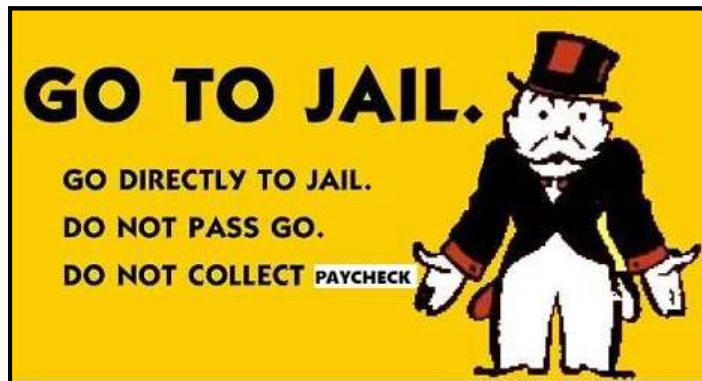
- Loss or compromise of classified or controlled sensitive information
- Weapons systems cloned, destroyed, or countered
- Loss of technological superiority
- Economic loss
- Physical harm or loss of life

Fighting the Insider Threat

DETER

DETER

To prevent an action by fear of consequences.



Take Annual Training!

Be Aware!

Read The Signs!

DETECT

DETECT

To discover, identify, or investigate the presence or existence of something.



Detecting potentially malicious behaviors



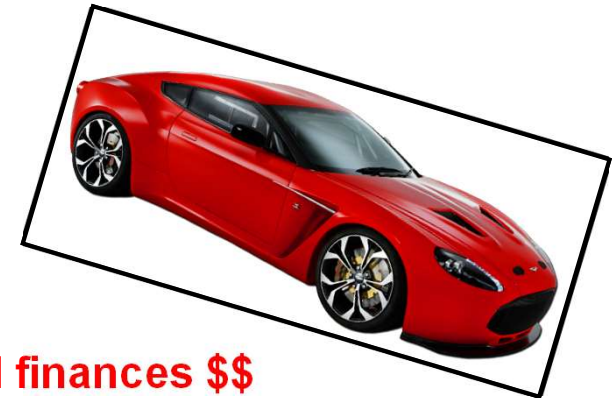
Taking classified information



Change in attitude



Unexplained finances \$\$



MITIGATE

MITIGATE

To make less severe, serious, or painful.



Self Report!



Take Annual Training!

Recognizing the Insider Threat

How to Recognize an Insider Threat



- Repeated security violations and a general disregard for security rules
- Failure to report overseas travel or contact with foreign nationals when required to do so
- Bringing an unauthorized electronic device into a controlled area
- Discussing classified info on a non-secure telephone or in non-secure emails or text messages
- Attempting to enter areas not granted access to or accessing information not needed for job
- Being disgruntled to the point of wanting to retaliate

Recognize the Insider Threat (continued)



Behavioral Indicators*

- Depression
 - Stress in personal life
 - Exploitable behavior traits:
 - Use of alcohol or drugs
 - Gambling
 - Financial trouble
 - Prior disciplinary issues
- * These behaviors may also be indicative of potential workplace violence.*



Reporting the Insider Threat

Who to Report to?

Each employee has a responsibility to ensure the protection of classified and CUI entrusted to them. Be aware of potential issues and the actions of those around you and report suspicious behaviors to:

- Supervisors
- Security element
- Insider Threat Manager
- Law Enforcement
- Military Department CI Organization(e.g., NCIS)
- FBI



What to Report?

- Keeping classified materials in an unauthorized location (e.g., at home)
- Attempting to access classified information without authorization
- Questionable downloads
- Using an unclassified medium to transmit classified materials
- Discussing classified info on a non-secure telephone or in non-secure emails or text messages
- Removing the classification markings from documents
- Unnecessary copying of classified material
- Sudden reversal of financial situation or a sudden repayment of large debts or loans
- Being disgruntled to the point of wanting to retaliate
- Repeated or unrequired work outside of normal duty hours
- Bringing an unauthorized electronic device into a controlled area
- Making threats to the safety of people or property
- Expressing loyalty to another country
- Concealing reportable foreign travel or contacts

Note: The above list of behaviors is not inclusive, it only depicts a small set of examples. While not all of these behaviors are definitive indicators that the individual is an insider threat, these actions should be reported before it is too late.

Insert appropriate Distribution or CUI statement here

Failure to Report

- Military: Punitive action under Article 92 (UCMJ)
- Civilians: Appropriate disciplinary action under policies governing civilian employees
- Contractors: DoD 5220.22-M, NISPOM

All: Could lead to dishonorable discharge, loss of employment, loss of access (clearance), fines or loss of wages, or imprisonment.

Insider Threat Cases

Reality Winner – NSA Translator pled guilty to leaking classified docs about Russian interference in the 2016 elections. Sentenced to 5 years 3 months in prison; released early in June 2021.



Bryan Martin – Navy sailor pled guilty to four counts of attempted espionage. Accepted over \$11K from an undercover FBI agent. Received dishonorable discharge, forfeiture of all pay and sentenced to 34 years in prison.



Stewart Nozette – Gov't scientist pled guilty to attempted espionage for providing classified info to a person he believed to be an Israeli intelligence officer. Sentenced to 13 years in prison.



James Michael Wells – US Coast Guard civilian employee received life sentence for killing two coworkers.

Jin Hanjuan - Software engineer stopped by DHS at Chicago airport. Had more than 1,000 classified electronic and paper docs. Sentenced to four years in federal prison for stealing Motorola trade secrets and fined \$20K; released on good behavior.



Insider Threat Cases

(continued)

Chelsea Manning (formerly Bradley Manning) – Responsible for unauthorized disclosure of classified info to WikiLeaks.



Nidal Hassan – Deadliest shooting on an American military base killing 13 people, injuring over 30 others.

Edward Snowden – Responsible for unauthorized disclosure of classified NSA surveillance programs.



Aaron Alexis – IT contractor responsible for killing 12 people at the Navy Yard.

John Beliveau – Former NCIS agent traded classified information in exchange for gifts and money.



Summary

IF YOU SEE SOMETHING



SAY SOMETHING

Questions



Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



CI & Insider Threat Awareness Brief

CAPT Todd Hutchison
Commanding Officer, NSWCCD

NCIS

Lawrence Tarasek
Technical Director, NSWCCD

NCIS

TYPES OF THREATS }



INADVERTENT

“Loose tweets sink fleets.” You do not have to intend harm to create a threat. Lack of OPSEC can lead to non-intentional disclosures.

Adversaries often exploit personnel's lack of OPSEC through the monitoring of social media sites, using elicitation, and eavesdropping.

1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N




NCIS

TYPES OF THREATS

FACT:

ADVERSARIES COLLECT SMALL PIECES OF INFORMATION.



WHEN COMBINED, THEY CAN REVEAL

THE WHOLE PICTURE

Source // Interagency OPSEC Support Staff, *Intelligence Threat Handbook*



FOREIGN INTELLIGENCE ENTITY

A foreign organization, person, or group that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, disrupt U.S. systems and programs, or gain a competitive edge.

Includes foreign intelligence and security services, international terrorist organizations, organized crime groups, and drug cartels.

1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



NCIS



TRADITIONAL METHODS

- OPEN SOURCES
- ELICITATION
- EAVESDROPPING
- RECRUITMENT

OVER 97 COUNTRIES

BOTH FRIENDS & FOES

target the United States seeking information and technology.

Source // NSA Threat Briefing, 2008

1.800.543.6289 NCIS.NAVY.MIL TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



NCIS

TRADITIONAL METHODS



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

OPEN SOURCES

- Al Qaeda Handbook encourages searching online for data about government personnel, officers, targets, etc.
- The Internet and other media are key sources of intelligence information
- Social networking sites, such as Facebook, Twitter, and blogs, are monitored and exploited

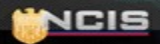
1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



NCIS

TRADITIONAL METHODS

ELICITATION

→ WHY IT WORKS THE ADVERSARY'S M.O. A SUBTLE DEFENSE

- GET you talking and KEEP you talking
- Common, effective technique to subtly collect information through face-to-face or online interaction
- Often used during facility and ship tours and at conventions and seminars where participants are eager to share information
- Operates under the guise of think tanks, exchange students, research organizations, foreign liaison officers, and official delegations



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

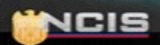
1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



NCIS

TRADITIONAL METHODS

ELICITATION

WHY IT WORKS

THE ADVERSARY'S M.O.

A SUBTLE DEFENSE

- Nonthreatening: Hard to recognize and easy to deny
- Easy to disguise: Seems like innocent conversation
- We're human: Exploits fundamental aspects of human nature. In general, we aspire to:
 - Be polite and helpful
 - Appear well-informed
 - Be appreciated
 - Trust others



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

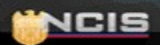
1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



NCIS

TRADITIONAL METHODS

ELICITATION

WHY IT WORKS

THE ADVERSARY'S M.O.

A SUBTLE DEFENSE

- Flattery/appeal to ego: Asks your opinion or values your insights
- Quid pro quo: Shares information with you in hopes you'll reciprocate
- Mutual interest: Focuses on details you have in common



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



NCIS

TRADITIONAL METHODS

ELICITATION

WHY IT WORKS

THE ADVERSARY'S M.O.

A SUBTLE DEFENSE

- Don't allow others to control the conversation
- Listen more than you talk
- Deflect a question with a question
- Change the topic
- Be general and nonspecific
- Plead ignorance
- Don't answer



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

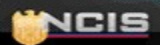
1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



NCIS

TRADITIONAL METHODS



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

EAVESDROPPING, ELECTRONIC SURVEILLANCE

- Operative positioned within earshot of a conversation or within view of a computer screen
- Communications intercepted when devices are connected to public Wi-Fi, unsecured networks, or unencrypted email systems

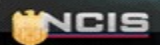
1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



NCIS

TRADITIONAL METHODS

RECRUITMENT

- Build personal relationship and gain trust, little by little
- Exploit personal weakness or circumstances
- Coerce or use inducements
- Start with small requests, then make bigger demands
- Praise and reward for accomplishments



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



OPSEC | REMINDERS

- ▶ Think before you talk and limit the information you post
- ▶ Never speak about sensitive info in public or on unsecured lines
- ▶ Shred sensitive information, including PII
- ▶ Never bring home classified information
- ▶ Create strong passwords for each account and change them often
- ▶ Update and use security software
- ▶ Follow the need-to-know principle
- ▶ Follow all security and IA policies



NCIS



OPSEC | REMINDERS

THE SEA AIR SPACE EXPO BRINGS DOD AND FOREIGN ENTITIES INTO A COMMON SPACE. PLEASE REPORT ANY SUSPICIOUS ACTIVITY TO NCIS AS SOON AS POSSIBLE. THINGS NCIS WILL NEED:

- A DETAILED DESCRIPTION OF THE INCIDENT, INCIDENT LOCATION, AND PERSONS INVOLVED
- ON OCCASION, PERSONNEL MAY BE PROVIDED WITH A BUSINESS CARD OR CONTACT INFORMATION, PLEASE PRESERVE THIS INFO

1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

UNCLASSIFIED

CI & INSIDER THREAT
AWARENESS AND REPORTING BRIEF



C A R D E R O C K D I V I S I O N



Questions



Carderock Division



SA DONALD KNIGHT

CELL: 202-714-9751

DESK: 202-433-3858

NIPR: donald.knight@ncis.navy.mil

SIPR: donald.knight@ncis.navy.smil.mil



Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



New Hires / Employee Initial Safety Brief

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Occupational Safety and Health Branch

Larry Tarasek
Technical Director, NSWCCD

Introduction

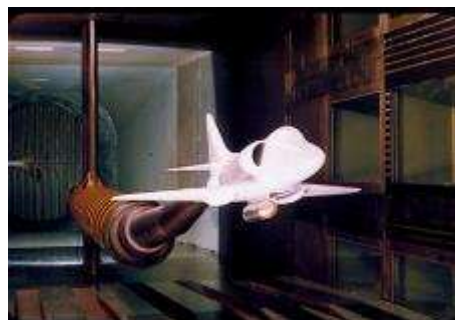
Our Goal

The Occupational Safety and Health Branch (safety office) and your leadership team is committed to ensuring you go home in the same condition as when you came into work.

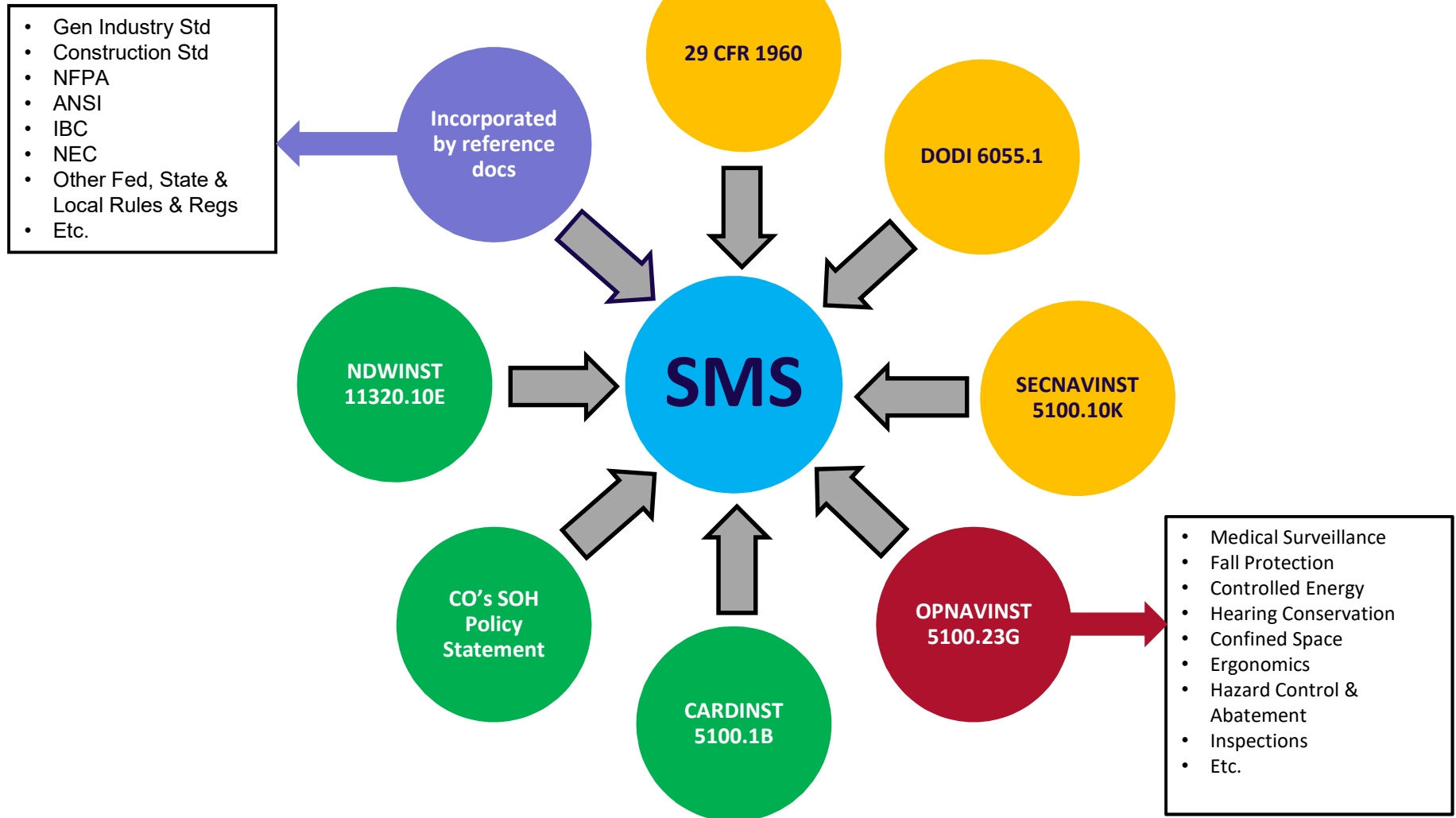


Introduction (Cont.)

- We obey OSHA standards.
- Safety is equally as important as any thing else you do here.
- Supervisor's will brief you on hazards/controls of your work area.
 - Including those who travel and are exposed to unfamiliar hazards



NSWCCD Safety Management System (SMS)



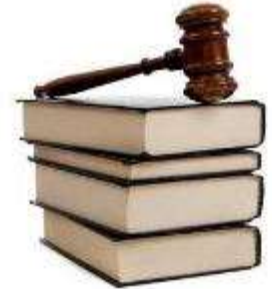
Initial Safety Training



- Must be trained to the hazards and controls in your work area
- After this initial familiarization your supervisor:
 - Provides/assigns specific training applicable to your job position
 - duty tasks
 - general safety required by all
 - OJT and other training based on resources available in the work area
 - May include Tier 1 Ship/Sub (Subsafe) requirements
- Once you acquire your CAC
 - Log into ESAMS and complete web based safety training (procedure included in your packet)
- Do not feel compelled/pressured to do anything you've not been trained on or feel uncomfortable/unsafe doing

OSH Act

- OSH Act signed by Nixon in 1970
 - Requires all employers to provide a safe and healthful workplace by:
 - Encouraging employers and employees to reduce workplace hazards through hazard recognition and mitigation
 - Providing education and training
 - Providing worksite evaluations
 - Informing employees of their rights and responsibilities (New hire brief and DON OSH Poster on bulletin boards)



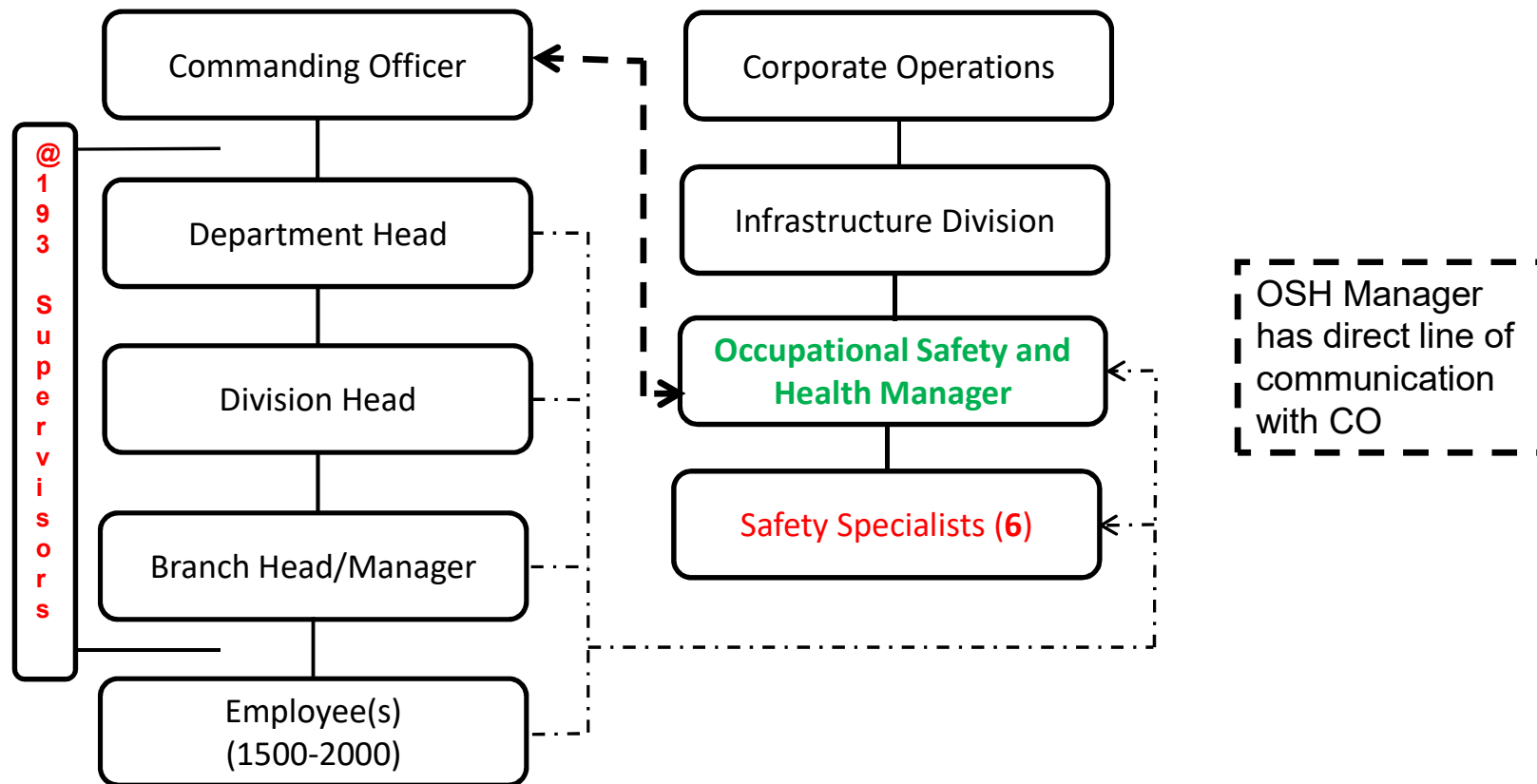
Roles and Responsibilities



- Supervisors and line management are responsible for the safety of their employees/workers.
 - Safety specialists are the COs technical experts on safety related matters
- Each of you is personally responsible to:
 - Work safely to help reduce unsafe/unhealthful working conditions, including unsafe acts.
 - Report hazards to your supervisor.
 - Stop work if you think its not safe.
 - Complete your assigned training.
 - Report injuries and illnesses to your supervisor (even off duty injuries). Also report medication which may impair your ability to perform your job.
 - Ask questions
 - Because we've always done it that way was doesn't mean it's the right way.
 - If not satisfied – contact safety.



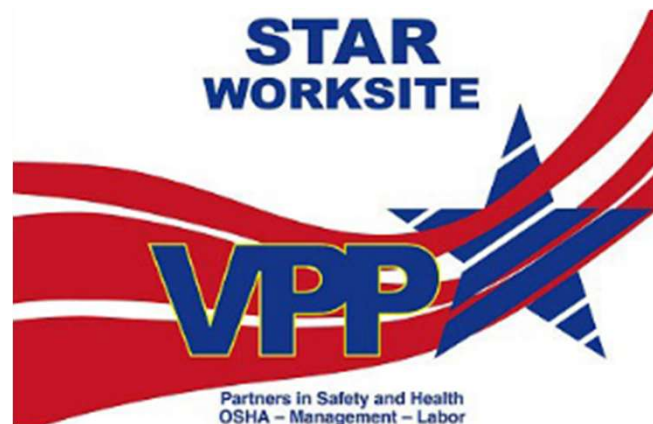
Safety Responsibility/Accountability Organization Chart



Voluntary Protection Programs (VPP)



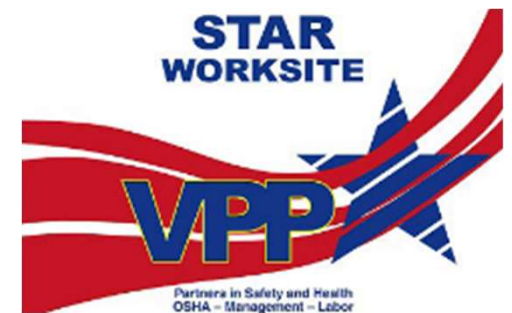
- **VPP is OSHA's recognition program for sites having an effective SMS.**
 - Highest safety award the US Government can bestow on a worksite.
 - Significant achievement - we are 1 of approx. 2300 worksites out of over 8 million worksites in the U.S.
 - Recertified VPP Star worksite November 2018



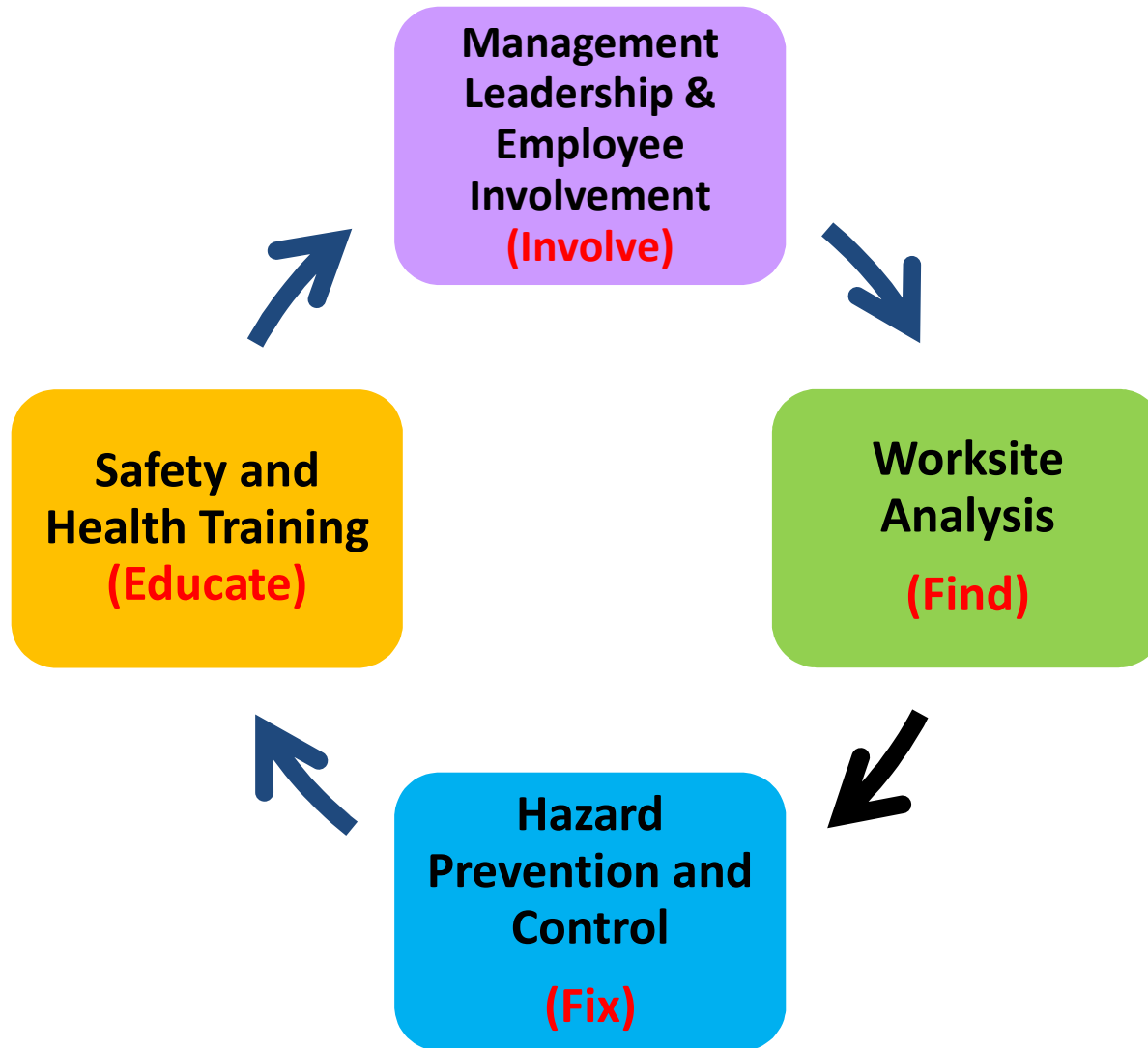
Voluntary Protection Programs (VPP) (Cont.)



- **Three voluntary protection programs**
 - **Site Based** (defined specific geographic location)
 - Mobile Workforce (majority of workforce is vehicle based, does not work in a stationary office)
 - Corporate (main office or HQ)
- **Two recognition levels for the programs**
 - **Star** (meets or exceeds all program requirements)
 - Merit (minor tweaks needed to meet the program requirements)



Four Elements of VPP



How Are We Assessed

Document Review

Written Programs

Supporting Documents

Interviews

Formal

Informal

Observation

Work Spaces

Non-Classified Operations

NSWCCD VPP Website

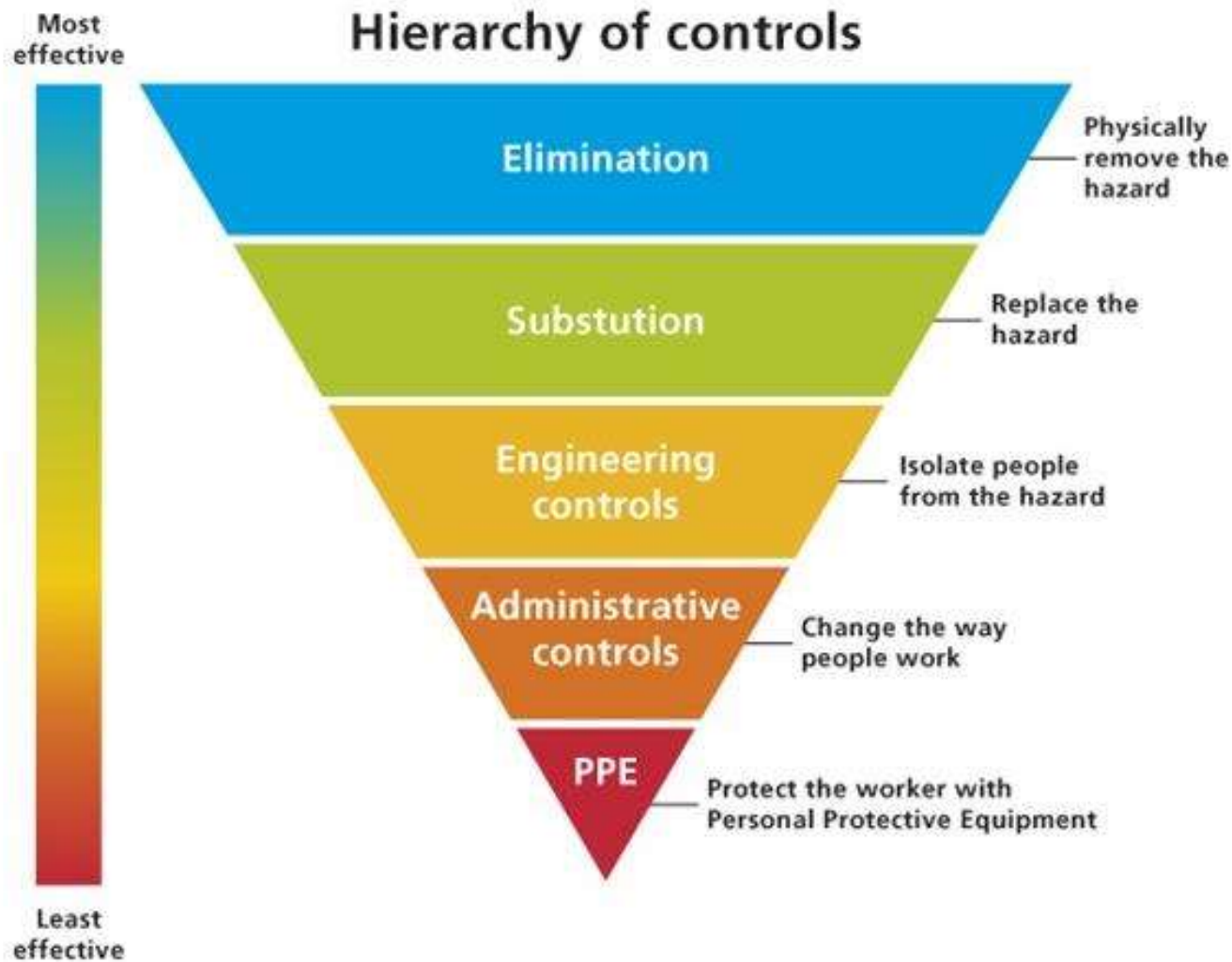


The screenshot displays the NSWCCD VPP website interface. At the top, there is a header with the NAVSEA logo and navigation links for 'EMPLOYEE DIRECTORY' and 'SITE INDEX'. Below this is a secondary navigation bar with categories like 'INTRANET TOOLS', 'BUSINESS INFO', 'COMPUTER INFO', 'EMPLOYEE INFO', and 'DOCUMENTS'. The main content area is divided into several sections:

- Quick Links:** A list of links including 'Carderock Call', 'Carderock Intranet Sites', 'DADMS & DTPR EOW', 'Desktop Quality Mgmt System (QMS)', 'DTI Travel', 'Maritime Technology Information Center (MTC)', 'Networking Web Page', 'Online Training', 'OPM Data Download', 'Organizational Charts', 'SharePoint Home', 'Technical Services', and 'Voluntary Protection Programs (VPP)'. The 'Voluntary Protection Programs (VPP)' link is circled in red with an arrow pointing to the right.
- Announcements:** A section titled 'Tuesday, Aug. 7' featuring 'Troy Topping' from California State University, Sacramento, and 'Jack Price and Judy Conley' from the USCG Santa Rosa. It also includes a calendar view for the month of August.
- Voluntary Protection Programs (VPP):** The main content area features a large header with the VPP logo and the title 'Voluntary Protection Programs'. Below this, there is a detailed description of the VPP program, its goals, and a list of five key elements: Management Leadership and Employee Involvement, Worksite Analysis, Hazard Prevention and Control, Safety and Health Training, and a fifth element partially visible. A 'Criteria' section follows, listing five specific requirements for VPP certification.
- Documents:** A list of documents including 'Commanding Officers Occupational Safety & Health Policy Statements', 'Preparing for the OSHA VPP Recertification', 'Site Hazard Identification Examples', 'New Hire Contractor and Visitor Handbook (Print two-sided. Flip on short edge)', 'OSHA OSHA Summary of Injuries and Illnesses 2015 - 2017', and 'Annual VPP self-...'.



Hierarchy of Hazard Controls



PPE

- Rx safety eyewear vendors – onsite monthly
- Footwear vendors - quarterly



PPE (Cont.)

- Personal Protective Equipment (PPE):
 - Emails announce dates/times
 - Your supervisor will provide all required PPE
 - Dress appropriately for your work environment:
 - No open toe shoes, sandals or flip flops are allowed in laboratory and shop spaces.
 - Wear protective footwear when required.
 - For your protection comply with all **SIGNS!!**



**You can eat with false teeth
You can't see with a glass eye**

Control Programs

- CPR/First Aid/AED

- 50 AEDs on site



- Fire Drills

- Traffic

- Comply with all local and state laws as well as posted speed limits
- Give way to emergency vehicles
- Do not stop on barriers at gate
- Pedestrians in cross walks have right of way
 - Make sure driver sees you



- Winter weather - walking on icy sidewalks, or driving on snow covered roads. (slips, trips and falls)

Review Handout

Shoreside or Shipboard Pocket Safety Guide

**Specifically – Confined Space, Fall Protection,
Energy Control (LO/TO), and HAZMAT/HAZCOM**

HAZMAT/HAZCOM

- All employees who work with hazardous materials (HAZMAT) shall receive training before working with any hazardous material per the hazardous communication (HAZCOM) standard 29 CFR 1910.1200.
 - Initial HAZCOM training via ESAMS and as directed by supervisor based on job tasks.
 - Covers changes implemented by Globally Harmonized System.
 - Revised labeling and SDS (8 to 16 sections, pictograms).



Safety Data Sheet (SDS)

- Provides information needed to safely use, store and dispose of hazardous materials.

WD-40 COMPANY
Safety Data Sheet

1 - Identification
Product Name: WD-40 Multi-Use Product Aerosol
NOT FOR USE IN CALIFORNIA
Product Use: Lubricant, Penetrant, Drive Out
Moisture, Removes and Protects Surfaces Free
Corrosion
Restrictions on Use: None Identified
SDS Date Of Preparation: 07/02/2014

2 - Hazard Identification
Hazardous (GHS) Classification:
Flammable Aerosol Category 1
(Gas Under Pressure: Compressed Gas
Respiration Toxicity Category 1)
Note: This product is a consumer product and is labeled in accordance with the US Consumer Product
Safety Commission regulations which take precedence over OSHA Hazard Communication labeling. The
actual consumer label will not include the label elements below. The labeling below applies to
industrial/professional products.
Label Elements:

DANGER:
Extremely Flammable Aerosol.
Contains gas under pressure; may explode if heated.
May be fatal if swallowed and enters airways.
Precaution:
Keep away from heat, sparks, open flames, hot surfaces – No smoking.
Do not spray on an open flame or other ignition source.
Pressurized container: Do not pierce or burn, even when empty.
Response:
IF SWALLOWED: Immediately call a POISON CENTER or physician. Do NOT induce vomiting.
Storage:
Store locked up.
Protect from sunlight. Do not expose to temperatures exceeding 50°C/122°F. Store in a well-ventilated place.
Disposal:
Dispose of contents and container in accordance with local and national regulations.

3 - Composition/Information on Ingredients

Ingredient	CAS #	Weight Percent	US Hazards 2012 GHS Classification
Aliphatic Hydrocarbon	8470-27-4	45-80	Flammable Liquid Category 2

Page 1 of 1

SAFETY DATA SHEETS ELEMENTS

- 1. IDENTIFICATION**
Includes product identifier; manufacturer or distributor name, address, phone number; emergency phone number; recommended use; restrictions on use.
- 2. HAZARD(S) IDENTIFICATION**
Includes all hazards regarding the chemical; required label elements.
- 3. COMPOSITION / INGREDIENT INFORMATION**
Includes information on chemical ingredients; trade secret claims.
- 4. FIRST-AID MEASURES**
Includes important symptoms / effect, acute/delayed; required treatment.
- 5. FIRE-FIGHTING MEASURES**
Lists suitable extinguishing techniques, equipment; chemical hazards from fire.
- 6. ACCIDENTAL RELEASE MEASURES**
Lists emergency procedures; protective equipment, proper methods of containment and cleanup.
- 7. HANDLING AND STORAGE**
Lists precautions for safe handling and storage, including incompatibilities.
- 8. EXPOSURE CONTROL / PERSONAL PROTECTION**
Lists OSHA's Permissible Exposure Limits (PELs); Threshold Limit Values (TLVs); appropriate engineering controls; personal protective equipment (PPE).
- 9. PHYSICAL & CHEMICAL PROPERTIES**
Lists the chemical characteristics.
- 10. STABILITY & REACTIVITY**
Lists chemical stability and possibility of hazardous reactions.
- 11. TOXICOLOGICAL INFORMATION**
Includes routes of exposure; related symptoms, acute and chronic effects; numerical measures of toxicity.
- 12. ECOLOGICAL INFORMATION**
Includes ecotoxicity, persistence and degradability; bio accumulative potential and mobility in the soil.
- 13. DISPOSAL CONSIDERATION**
Describes waste residues and information on their safe handling and methods of disposal, including the disposal of contaminated packaging.
- 14. TRANSPORT INFORMATION**
Includes UN number and proper shipping name; transport hazard class(es); packaging group; environment hazards.
- 15. REGULATORY INFORMATION**
Includes safety, health and environmental regulations specific for the product.
- 16. OTHER INFORMATION**
As needed.
Reorder: GHS-19604 www.ComplianceSigns.com

GHS Pictograms

FLAMMABLE CORROSIVE EXPLOSIVE

COMPRESSED GAS OXIDIZING TOXIC

HEALTH HAZARD HARMFUL/IRRITANT DANGEROUS FOR THE ENVIRONMENT

Report Hazards



See Something, DO Something!

- Report to Supervisor (follow-up) (can do anonymously)
- Unsafe/Unhealthful Form (ESAMS/Bulletin board)
- Email safetynswccd.fct@navy.mil
- Facilities Service Desk (301-227-1330)
- Notify Departmental Safety Rep/COI
- Contact Safety Branch POC

Potential Exposures



- Older buildings may have intact stable asbestos or man-made vitreous fibers (MMVF)
- If any surface is accidentally damaged/exposed (especially in old buildings):
 - Do not disturb the exposed material
 - Secure any fans/blowers/doors in the areas which may cause the material to become airborne
 - Contact your supervisor and the safety branch immediately



Occupational Health



- Occupational Health Clinic is located at Walter Reed Medical Military Medical Center (WRNMMC) in Bethesda, MD. (9 miles)
 - Medical surveillance programs
 - Supervisor provides Form 5100/1T generated by ESAMS
 - Must bring signed form back to supervisor
 - Audiology services - hearing conservation program (base line)
 - Certification exams - Pre-placement exams to determine if you are fit for duty or medically qualified for your job.
 - Physical for respirator (we provide fit testing and respirator after physical completed)
 - Industrial Hygienists
 - Conduct workplace surveys
 - Spot checks
 - As requested investigations



Occupational Health (Cont.)

- During Heat Stress Conditions

- Flags are no longer flown but “All Hands” notices are posted on the NSWCCD Intranet home page to indicate heat conditions when appropriate (starting w/ temps >80 WGB).




Occupational Health (Cont.)



- RODS (Recreational Off-Duty Sports)
 - Black Flag Release Waiver Form - Prior to engaging in Employee Services Association (ESA) sponsored athletic activities during Black Flag conditions, participant must obtain and complete the Black Flag Waiver Form and submit it to ESA, where it will be maintained.

NSWCCD EOSH - Web Access



CARDEROCK DIVISION INTRANET

Code: 00 | 01 | 02 | 10 | 60 | 70 | 80

EMPLOYEE DIRECTORY | SITE INDEX

INTRANET TOOLS BUSINESS INFO COMPUTER INFO EMPLOYEE INFO DOCUMENTS

Quick Links

- Carderock Café
- Carderock Intranet Sites
- DADMS & DITPR-DON
- Division Quality Mgmt System (QMS)
- DTS Travel
- Maritime Technology Information Center (MTIC)
- Mentoring Web Page
- Online Training
- OPM Data Breach
- Organizational Charts
- SharePoint Home
- Technical Services

Employee Toolbox

- Base Maps
- Communications Toolbox
- 2017 Payday & Holiday Schedule/Calendar
- Carderock Brochures
- Emergency Action Quick Reference Guide
- Photo Gallery
- Shuttle Bus & Transit Info

Check it out! Carderock's Year in Review 2016

Click Here

Announcements

- West Bethesda - MTIC Parking Lot restriction, May 1
- West Bethesda - Carderock's Professional Societies Day, May 3
- Division - Voluntary Leave Transfer Program Update as of April 24
- West Bethesda - National Day of Prayer, May 4
- West Bethesda - Prescription safety eyewear opticians visit, May 4
- Division - Mandatory DON EEO Training Notice: Available in TWMS or Face to Face Training (next session May 11)

From the Top

- Captain Mark Vandroff, USN
Commanding Officer
- Dr. Joseph T. (Tim) Arcano, Jr.
Technical Director

Got a question or comment for leadership? Send an email to the leadership mailbox.

[Leadership Mailbox](#)

INCLEMENT WEATHER GUIDANCE

fusion

milSuite

FORCE PROTECTION CONDITION BRAVO

WAVES Fall 2016

Wavelets

CARDEROCK DIVISION INTRANET

NAVSEA

Where the Fleet Begins

INTRANE

Quick Links

- Carderock Café
- Command Intranet Sites
 - Board of Directors (BOD)
 - Code 00 - Division Command
 - Code 01 - Office of the Comptroller
 - Code 02 - Contracting & Acquisition Department
 - Code 10 - Operations Department
 - Code 60 - Survivability, Structures, Materials & Environmental Department
 - Code 70 - Ship Signatures Department
 - Code 80 - Naval Architecture & Engineering Department
 - Code 90 - Machinery Research & Engineering Department
 - Cyber Security Program
 - Facilities & Model Fabrication
 - Environmental & Occupational Safety & Health (EOSH) Office
 - Human Resources Office
 - Investment Portfolio
 - Naval Criminal Investigative Service (NCIS)
 - NMCI
 - Security Office



NSWCCD EOSH - Web Access (Cont.)



Code: 00 | 01 | 02 | 10 | 50 | 70 | 80
EMPLOYEE DIRECTORY | SITE INDEX
INTRANET TOOLS | BUSINESS INFO | COMPUTER INFO | EMPLOYEE INFO | DOCUMENTS

[Home](#) > [Corporate Operations](#) > [Environmental & Occupational Safety & Health Office](#)

- Environmental Management System (EMS)
- HAZMAT
- Personal Protective Equipment (PPE)
- Supervisors
- Training
- MEI (MS) Property Damage/Near Miss
- Safety
- Voluntary Protection Program (VPP)
- EOSH Goals/Commitments
- Explosives Safety
- Environmental Alerts
- Safety News



Environmental & Occupational Safety & Health (EOSH) Office

The Environmental and Occupational Safety and Health (EOSH) Office is responsible for regulatory compliance for both Environmental programs and Occupational Safety and Health programs. This office is responsible for providing assistance with and oversight of compliance with applicable environmental, occupational safety, radiation safety, and explosives safety requirements throughout the West Bethesda Site and its subelements.

The EOSH maintains personnel and offices in West Bethesda, MD, Little Creek, VA, and Dayton, ID. Program support is provided to the Carderock Division's other deployment sites through the EOSH staff and resources.

- ### Contact Information
- Safety Office (301) 227-1510
 - Environmental Office (301) 227-1892
 - [Resources & 2](#)
 - [Programs & 3](#)
 - West Bethesda POCs

- ### Travelers
- - [Click to View](#)
 - [Back Logging Master List](#)

- ### News
- The Occupational Safety and Health Office (OSHA) has a new consolidated e-mail address: NAVCCD.Safety.Office@navsea.mil
 - Feel free to use it if you have general questions, suggestion, feedback, and submit to medical surveillance documentation (in case to make message and attachments appropriate), need ES&MS help, etc. We look forward to hearing from you.
 - POC is OSH Branch Head Andrew Gagnatova at 227226.00030202@navsea.mil or 301-227-3011



- ### Useful Links
- Check Authorized User List (AUL)
 - Disposal of Hazardous Waste (including ballistics)
 - SDS or MSDS (Need to know 2/1/10)
 - ESHMS
 - On Line Safety Training
 - OSHA Standards
 - Report Unethical/Unethical Working Conditions (USAWC)
 - Report Unethical/Unethical Working Conditions (Form) (WARNING: It is extremely dangerous to fill or copy. Immediately contact your supervisor, or call the OSH Office at 227-1510)

- ### Instructions & Documents
- Occupational Safety & Health Policy Statement
 - Inspection of Portable Air Conditioners
 - CARDEROCKDIV/NAV-3100-1A
 - NAV-226-200-1 3/10/140
 - NAV-226-200-1 3/10/140 (OH 1)
 - NAV-OSH 3100-250 (OH 1)
 - Procurement Authorization (PAC)
 - Training
 - Water Based National Military Medical Center (WBNMCC) Industrial Hygiene

- ### Forms
- Job Hazard Analysis (JHA) Form
 - Job Hazard Analysis (JHA) Checklist
 - JHA Development Training Presentation
 - Hazard Team Protocol
 - O3 Form 2273



Environmental

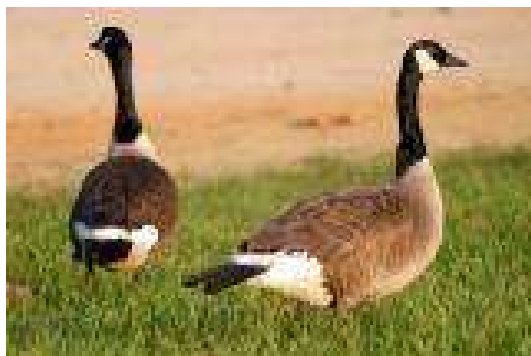
- CO's Environmental Policy statement is in your packet.
- Federal, state and Navy environmental regulations apply on base. Do not pour anything down any drains, sinks, or on the ground.
- In case of any type of spill attempt to safely isolate/contain the spill and contact the Environmental Office (Code 1023) at [\(301-227-1892/1510\)](tel:301-227-1892/1510)
- If you cannot do so safely, contact the emergency number [\(202- 433-3333\)](tel:202-433-3333) for proper removal/disposal. Report your installation (Carderock), building #, your name and emergency type/info.



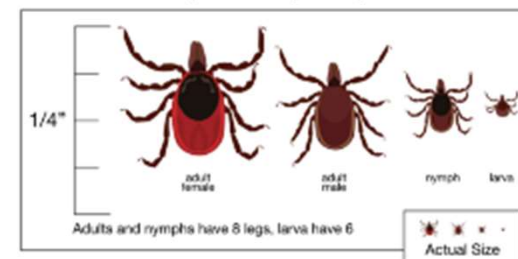
Environmental (Cont.)



- Park only in designated areas - not off road, on the grass, or under trees.
- We have several wildlife species here, do not feed geese or other wildlife.



How to Identify Black Legged or Deer Ticks (*Ixodes Scapularis*)



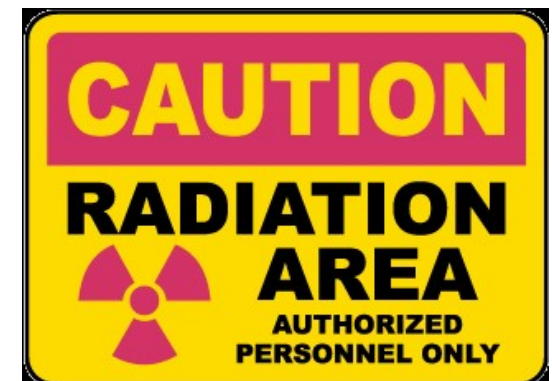
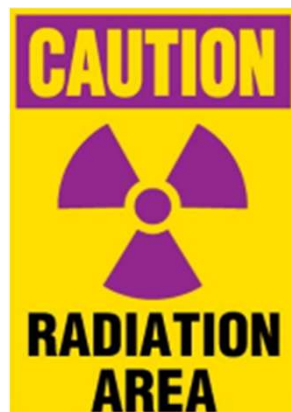
Radiation Affairs Support Program (RASP)



- Training for Members of the Public and Other Organizational Personnel Working in Proximity to RASP Controlled Areas
- Anyone not in the RASP is considered a member of the public
- Training ensures you can:
 - Recognize radiation hazard areas
 - Know what to do when you see them
 - Understand radiation dose requirements
 - Know who to contact for more information

RASP Safety Training (Cont.)

- Variety of radioactive materials and radiation producing devices/sources used in support of science, engineering, R&D
 - Audits/surveys routinely conducted of operations to ensure safety of the public.
 - Personnel working in these areas are monitored by dosimeter
- Obey warning signs - Ionizing radiation warning signs have a magenta trefoil with a yellow background



Types of Radiation

- Non-ionizing radiation – lasers, radiofrequency (RF) emitters, visible light – sunlight, indoor lighting (does not change cell structure or DNA - normally not harmful)
- Ionizing radiation- radioactive sources/x-ray devices, gamma and all particle radiation from radioactive decay (may cause change to cell structure or DNA - harmful under conditions)

Radiation Dose

- Per NAVMED P-5055, the annual exposure limit for radiation workers is **5,000 mrem p/yr**. Per RAD-010, the Navy has further reduced the annual limit for these workers to **500 mrem p/yr**.
 - Radiation exposures which were compliant with these annual limits have been scientifically proven to cause no injuries to man.
- While working adjacent to these areas at NSWCCD your radiation dose **will not** exceed **100 mrem** in a year from RASP-controlled sources. (Equivalent to normal sunlight exposure per year)

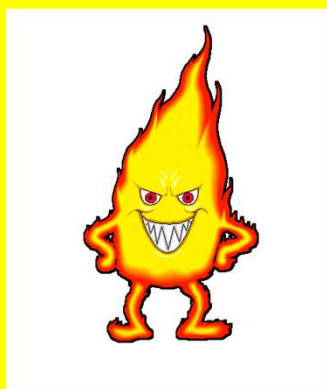
RASP Points of Contact



- Who should I contact if I have further questions?
 - Your supervisor.
 - The applicable Facility Manager.
 - Radiation Safety Office at 301-227- 2316 or 3014/4584/1510.

Emergencies

To report a fire, hazardous materials spill or medical emergency call **202-433-3333** and notify your supervisor.



Our on-base Fire Department/EMT and Security services will dispatch and respond to your call.

DO NOT DIAL 911. Call 202-433-3333.

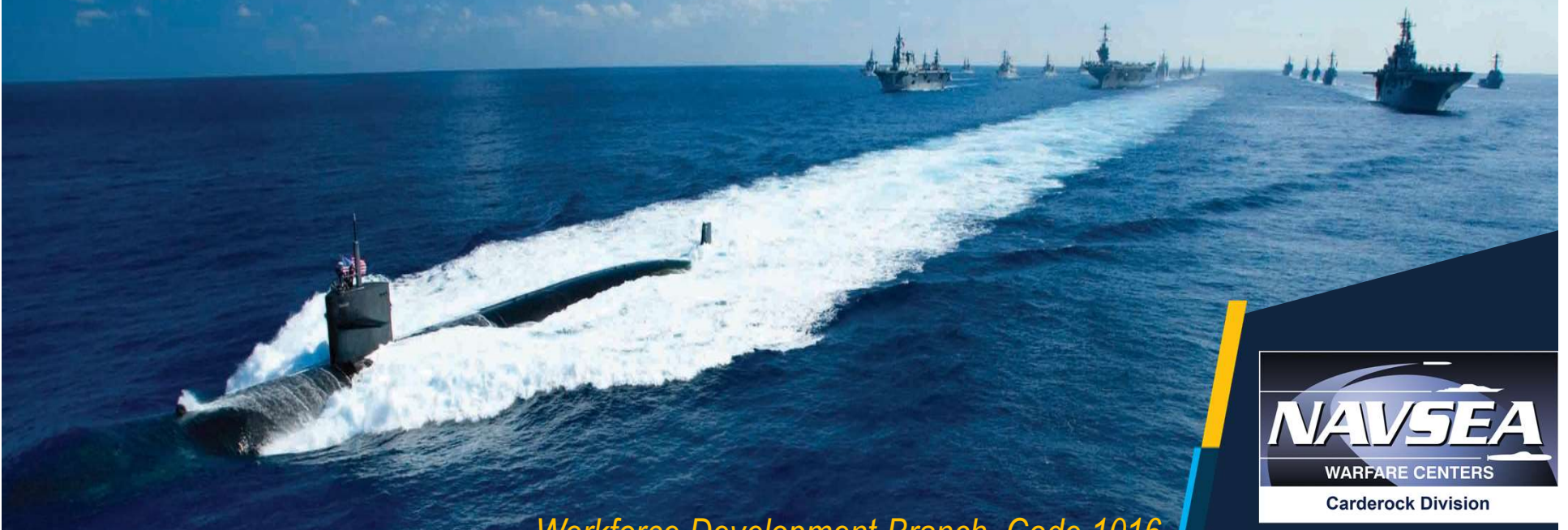
YOUR Role



- **Review the handouts**
- **Comply with SMS**
- **Focus on safety**
 - Integrate safety into what you do
- **Plan to work safely**
 - Know what the risks are
- **Don't accept non-compliance as the norm**
- **Every workplace has hazards**
 - Know yours
- **Set a good example and get involved**

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



Workforce Development Branch, Code 1016



WFD 2-Day Onboarding Brief

Topics



- Mission
- Workforce Development Branch Point of Contacts
- Ad-Hoc Training Requests (ATR)
- Total Workforce Management Services (TWMS)
- Mandatory Training
- Supervisor Mandatory Training
- Leadership Development Programs
- Carderock 101
- Onsite Command Wide Training
- Onboarding Follow-Up

For more information, go to:

[Carderock HR WFD – Intranet Page](#) or [Carderock HR WFD – Wiki Page](#)



Mission



Provide high quality, timely and relevant employee development programs that enhance individual knowledge, skills and abilities.

Develop employees that have the skills that allows the division to meet our customers needs.

Provide programs that develop a well-rounded employee.



Workforce Development Branch Point of Contacts



Jorge Galindo

jorge.l.galindomelecio.civ@us.navy.mil

(301) 742-9701

Training Officer - Workforce Development Branch
Head

Linda Florian

linda.k.florian.civ@us.navy.mil

(301) 204-4146

Approving Official for WFD Purchase Card Holders
Program Manager for DAWIA, Onsite Training,
Scientist Engineer Development Program (SEDP),
Extended Training ETT Program

Olamidayo Diana Odusanya

olamidayo.d.odusanya.civ@us.navy.mil

(240) 274-9362

Training Purchase Card Holder - Code 80
Program Manager for Leadership Development
Programs Carderock 101

Renard Walker

renard.c.walker.civ@us.navy.mil

(301) 318-4285

Training Purchase Card Holder - Code 70, Code 02
Program Manager for Mandatory Training, LinkedIn

Cecelia Paulding

cecelia.g.paulding.civ@us.navy.mil

(240) 274-9702

Training Purchase Card Holder - Code 60
Program Manager for Individual Development Plan
(IDP)
Defense Acquisition Workforce Improvement Act
(DAWIA)

Jeffrey Klimczak

jeffrey.a.klimczak.civ@us.navy.mil

(301) 275-2517

Training Purchase Card Holder - Code 00, Code 01,
Code 03, Code 10, NSWC/NUWC HQ
Program Manager for Supervisor Training, PROPEL
Carderock University, NPS

Ad-Hoc Training Requests (ATR)



- How to access & learn about potential training - All Hands Emails, TWMS, Carderock Intranet, Course Catalog, Internet
- Must be entered into Navy Enterprise Resource Program (ERP) ERP NLT three weeks prior to class start date; Navy ERP Link: [Enterprise Resource Program \(ERP\)](#)
- Submit support documents
 - (Approved Individual Development Plan in TWMS invoice, quote, account info., etc.)
- Do NOT attend training until fully approved
 - Workforce Development is final approval
 - Attending course with approval constitute an Un-authorized Commitment (UAC) violation
- **Training requests received after the employee is enrolled and/or begins training without the appropriate approvals is an **Unauthorized Commitment (UAC)**.**
 - In this situation, the training request will be sent to Code 02 for UAC processing. Employees who enroll in training without prior approval will be held responsible for the total cost of the training.
- No-Show – Department still pays (employee may be require to payback training cost)
- Provide proof of training completion



For more information, check out:

[Ad Hoc Training Request Process - Workforce Development Page - NAVSEA Wiki \(navy.mil\)](#)

Total Workforce Management Services (TWMS)



Total Workforce Management Service (TWMS) is a government application which gathers information from a number of official programs of record and combines all this data to allow the user to manage their workforce via one easy-to-use web interface. TWMS provides employees access to a number of training courses and allows them to view their personnel information such as Notifications of Personnel Action (SF50s).

To access TWMS, employee must have a Common Access Card (CAC) Access. [TWMS: Total Workforce Management Services \(TWMS\)](#)

[Total Workforce Management Services \(TWMS\) Quick User Guide](#)

Total Workforce Management Services (TWMS)
Workforce Manager 2.0 //

** FOR OFFICIAL USE ONLY - PRIVACY ACT SENSITIVE **
** Any misuse or unauthorized disclosure of this information may result in both civil and criminal penalties **

NAVIGATION:

- HOME
- Login/Logout
- Information:**
 - Contact Us
 - Data Update Status
 - Employee Locator
 - Documentation & Training - New
 - TWMS Updates
 - Privacy Act Statement

Log into TWMS Workforce Manager

SELECT PROFILE: [dropdown]
SUBMIT

Click here for an Account Application

Click Here for Self-Service/myTWMS (Access your own record only)

Click Here to access TWMS Employee Locator

DoD Disclaimer

You are accessing a U.S. Government(USG) information system (IS) that is provided for USG-authorized use only.

By using this IS, you consent to the following conditions:

- The USG routinely monitors communications occurring on this IS, and any device attached to this IS, for purposes including, but not limited to, penetration testing, COMSEC monitoring, network defense, quality control, and employee misconduct, law enforcement, and counterintelligence investigations.
- At any time, the USG may inspect and/or seize data stored on this IS and any device attached to this IS.
- Communications occurring on or data stored on this IS, or any device attached to this IS, are not private. They are subject to routine monitoring and search.
- Any communications occurring on or data stored on this IS, or any device attached to this IS, may be disclosed or used for any USG-authorized purpose.
- Security protections may be utilized on this IS to protect certain interests that are important to the USG. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the USG. These protections are not provided for your benefit or privacy and may be modified or eliminated at the USG's discretion.

Mandatory Training



Training mandated by executive order, Federal statute, regulation or at the direction of the Secretary of the Navy is referred to as mandatory training and is required to be completed by all civilian employees on a reoccurring basis. Additional training may be required to be completed by supervisors and new Employees.

TWMS is the location to complete all non-safety related mandatory training. Training is announced via All Hands email and once the training is completed, employee's TWMS training record is updated accordingly.

To learn more, go to about this program:

[Mandatory Training – Workforce Development Page - NAVSEA Wiki \(navy.mil\)](#)

Checklist

Mandatory Training FY 22

Civilian employees must take all courses
Contract employees must take only those marked with an * and colored green



Training	Due	ID
<input type="checkbox"/> FY22 NAVSEA Active Shooter Training*	12/31/21	TWMS-667121
<input type="checkbox"/> FY22 DoD Cyber Awareness Challenge*	07/31/22	DOD-IAA-V19
<input type="checkbox"/> FY22 Privacy and Personally Identifiable Information (PII)*	09/30/22	DON-PRIV-2.0
<input type="checkbox"/> FY22 SAPR Refresher Training	09/30/22	TWMS-691361
<input type="checkbox"/> FY22 Records Management*	09/30/22	DOR-RM-010-1.2
<input type="checkbox"/> FY22 Workplace Violence Prevention	09/30/22	TWMS-656532
<input type="checkbox"/> FY22 Combating Trafficking in Persons (CTIP)	09/30/22	DOD-CTIP-5.0
<input type="checkbox"/> FY22 NAVSEA Counterintelligence Awareness (CIAR) Training*	09/30/22	DON-CIAR-1.0
<input type="checkbox"/> FY22 Annual Security Refresher*	09/30/22	TWMS-661607
<input type="checkbox"/> FY22 Operations Security (OPSEC)*	09/30/22	NOST-USOPSEC-4.0
<input type="checkbox"/> FY22 Anti-terrorism Training*	09/30/22	CENSECFOR-AT-010-2.0
<input type="checkbox"/> FY22 NAVSEA Derivative Classification Training	09/30/22	TWMS-571920
<input type="checkbox"/> FY22 Prevention of Sexual Harassment	09/30/22	TWMS-613963
<input type="checkbox"/> FY22 No FEAR Act	Biannually	TWMS-613957
<input type="checkbox"/> FY22 NAVSEA Intro to Controlled Unclassified Information*	09/30/22	TWMS-686594
<input type="checkbox"/> FY22 Time & Attendance Training	03/31/22	TWMS-693475



Supervisor Mandatory Training



Carderock has developed a toolkit that provides information regarding several supervisor training requirements and programs created to meet those requirements.

Propel Launch: This is a 5-day course that provides an introductory level awareness of NAVSEA expectations for **new first-line supervisors** at the Warfare Center Divisions, NAVSEA HQ, PEOs and Field Activities:

- Must be completed within **first year** of supervisory assignment. Courses are held monthly at 1 of the 10 Warfare Centers or NAVSEA HQ, either in-person or virtually.
- The student's home Division covers the labor and any travel costs required for the student to attend Propel. How the Division chooses to allocate these costs is at their discretion. There is no tuition or registration cost associated with the Propel training

Carderock Supervisor Program (CSP): CSP will satisfy the annual requirement for the year with the exception of DON USERRA and if taken as a refresher course will satisfy the requirement for a three-year cycle.

For more information about Supervisor Mandatory Training requirements, please visit our Supervisor Toolkit wiki page below: [Carderock WDP Supervisor Toolkit](#)



Leadership Development Programs



Carderock is dedicated to building new leaders and transforming leaders to better service our missions. To keep in line with this goal, various Leadership Development Program opportunities are available for employees to enhance their leadership skills and abilities. These programs are grade specific and vary in program duration.

To learn more about these programs or for latest updates, go to:

[Carderock Advanced Leadership Development Programs - Workforce Development Page - NAVSEA Wiki \(navy.mil\)](#)



Advanced Leadership Development Programs

The Department of the Navy (DoN) developed the following Leadership Program frameworks for Navy Personnel to obtain successful leadership skills through progressive learning. The Leadership Development Programs listed below are grade specific and vary in program duration. Also, it may be helpful to review the DoD Civilian Leader Development Framework to view a list of key competencies involved in being a leader. If you are interested in applying for a program, please click on the program name for additional information and follow the respective application instructions. Please ensure you also review all requirements and submit your application to Olamidayo Odusanya by the deadline as listed below.

⚠ If you are interested in applying for any of these programs, please submit your application by the specified date. Submitting your package early helps to ensure you meet the official program deadline. Your nomination package must be submitted via the appropriate chain of command. For quick checklist

DO NOT USE THE DEADLINES ON THE OCHR WEBSITE OR NAVSEA'S SHAREPOINT/WIKI PAGES.

For additional information/questions please email [Olamidayo Odusanya](#).

Program Name	Scope	Grade Eligibility	Carderock Application Due	Start Date	Program	Full/Part Time	Location
--------------	-------	-------------------	---------------------------	------------	---------	----------------	----------

Carderock 101



The purpose of this training is to inform interested employees about Carderock's mission and to give them a better understanding of how each Carderock department supports that mission.

Note: SEDP employees are required to complete this training.

Information about Carderock 101 training session dates, location, and registration process will be provided via ALL Hands by Public Affairs Office (PAO)



Onsite Command Wide Training



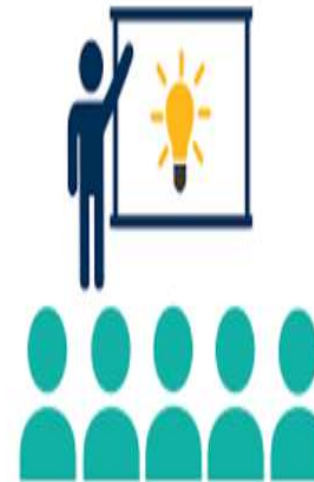
The Workforce Development Branch offers a variety of on-site training courses that have been created to develop and maintain a capable, diverse, and highly-motivated workforce.

Courses are held from 0800 to 1530; half-day classes are conducted from 0800 to 1200 unless otherwise specified.

To learn more, contact Workforce Development Branch or go to [On-site/Virtual Command-Wide Training - Workforce Development Page - NAVSEA Wiki](#)

On-site/Virtual Command-Wide Training

Created by Rebekah Knodel, last modified by Renard Walker on Sep 27, 2021



Course Schedule	Course Descriptions	Project Management Fundamentals	Project Management Principles	Microsoft Excel	Resume Building	Coaching and Mentoring
-----------------	---------------------	---------------------------------	-------------------------------	-----------------	-----------------	------------------------

Onboarding Follow-up



During Onboarding Follow-up Session, WFD program managers will be available to provide information and share updates about the programs below:

- Mentoring Program and Opportunities
- Individual Development Plan (IDP)
- Defense Acquisition Workforce Improvement Act (DAWIA)
- Scientist Engineer Development Program (SEDP)
- Extended Term Training (ETT) Program



Questions?



Wrap up

