
Department of the Navy
Information Security Standards Training
DATE 5-8-2023
Office of the Deputy Under Secretary of the Navy (Intelligence and Security)

Message from the Secretary of the Navy

Hon. Carlos Del Toro (far left), Secretary of the Navy, and key staff participating in the Department of the Navy Information Security Standards Training on May 8, 2023. (Navy photo by Mass Communication Specialist 2nd Class T. Logan Keown)

The recent unauthorized disclosure of classified information garnered the attention of our nation, who trust us to protect information critical to our national security. All leaders have a responsibility to understand the potential impact of these events and the importance of ensuring Sailors, Marines, civilians and contractors understand their roles in protecting classified information, in all forms, from unauthorized disclosure. Leaders must exercise extreme diligence to ensure this training is executed with the attention required to avoid further incidents. Additionally, we must continuously evaluate each person's responsibilities and "need-to-know" for access to classified information.

Security: All Hands on Deck

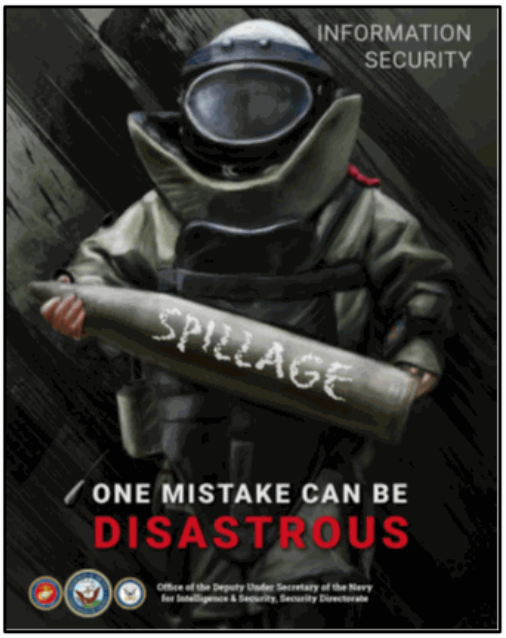
- Security requires an ALL HANDS commitment to protect our information.
- A strong security culture begins at the top!

Information Security = National Security

A Legal and Ethical Responsibility

- Unauthorized disclosure of classified information can adversely affect our national security and may result in criminal, civil or administrative sanctions.

- Never reveal or discuss classified information with anyone who does not have an active security clearance and a valid need to know.



Individual Responsibility

- You are responsible for:
  - Honoring your commitment to protect Classified National Security Information.
    - Non-Disclosure Agreement: A contract between you and the government that creates a lifetime contractual obligation for you to protect classified information.
  - Knowing your local security regulations pertaining to your assigned duties.
  - Notifying your Security Official(s) of changes in your status, which could affect your security clearance.
- Failure to protect can result in criminal or administrative sanctions:
  - Espionage Act of 1917 (can result in fine, incarceration or death) and the Hiss Act of 1954 (potential loss of retirement benefits).
  - Uniform Code of Military Justice

You are accountable for your actions and inaction.

Classified Information Access

SECURITY CLEARANCE

Administrative action, usually involving a form of background investigation and adjudicative determination.

+

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.

+

NON-DISCLOSURE AGREEMENT

Lifelong contract between the U.S. Government and you to protect classified information.

=

ACCESS

The ability and opportunity to obtain knowledge of classified information. This can involve seeing, hearing, or touching classified information, material, or equipment.

Without all three parts of the equation, there is no access to classified information.

What is an Unauthorized Disclosure?

The communication or physical transfer of classified to an unauthorized recipient.

- Everyone working with classified information is personally responsible to protect that information from unauthorized persons
- An unauthorized disclosure of information DOES NOT automatically declassify the information

Do not remove from a properly secured environment
Do not discuss outside of secure communication channels or properly secured environment
Do not try to "talk around" a classified topic
Do not copy, print, save, transcribe, photograph, or "screen shot" classified material without permission or outside the scope of your duties
Do not share or comment about your job or what you know on social media

Each Unauthorized Disclosure Damages our national security and puts our people at risk.

Reporting Insider Threat Behaviors

- Unexplained affluence
- Keeping unusual work hours
- Divided loyalty or allegiance to the U.S.
- Disregarding security procedures
- Unreported foreign contact and travel
- Pattern of lying
- Attempts to enlist others in illegal or questionable activity
- Verbal or physical threats
- Inquiry about operations where no need to know exists
- Fraud/Waste/Abuse of government credit cards or government equipment

If you see something, say something.

The reporting process protects you and the organization and is a responsibility for every member of the DON.

Your report may neutralize an insider prior to them going down a wrong path.

Report potential threats to your chain of command or to your service insider threat hub.

Navy Insider Threat

insiderthreat.fct@navy.mil

Marine Corps Insider Threat

insiderthreat@usmc.mil

Reporting Security Incidents

- ***Security Incidents***
  - All personnel who become aware of the loss or potential compromise of classified national security information are required to **immediately** report such information to security personnel and your chain of command. **Failure to report incidents may make you culpable for violations or compromises.**
    - Concerning behavior to your chain of command, local Insider Threat Program Manager.
    - DON Personnel may also report incidents to the Navy Inspector General.
    - Unauthorized Disclosure customizable briefing and Job Aids are available on the CDSE website.
    - Security incidents to Activity Security Managers (ASM) and / or Special Security Officers (SSO), Government Special Access Program (SAP) Security Officers (GSSO), as applicable, and their supervisors.
    - Security incidents involving IT to your information system security managers (ISSMs).
- ***Personnel Security***
  - Report, as soon as possible, potentially adverse or adjudicatively relevant information to your activity security manager or special security officer.
  - Commanders or security professionals will report credible information of adjudicative concern and any actions taken or anticipated within 72 hours to the appropriate adjudication facility.

Do not hesitate, early reporting may mitigate potential impacts.

When in doubt, report it!

Top Secret Information Accountability

- ***Accountability***
  - Top Secret information will be accounted by the Activity Security Manager. Optionally, Top Secret Control Officers (TSCO) *may* be appointed to facilitate Top Secret accountability.
  - The TSCO will develop and maintain a system of accountability for physical Top Secret documents and other media.
  - The system of accountability will document the following:
    - Receipt
    - Reproduction
    - Transfer
    - Transmission
    - Downgrading
    - Declassification
    - Destruction
  - Inventories of hard copy Top Secret material will be conducted at least once annually.
  - Classified material accountability records will be maintained for 7 years after the current calendar year.
  - Contact your local ASM, GSSO, or SSO for additional information.

If you are physically handling Top Secret material, ensure you are familiar with your local procedures and accounting requirements.

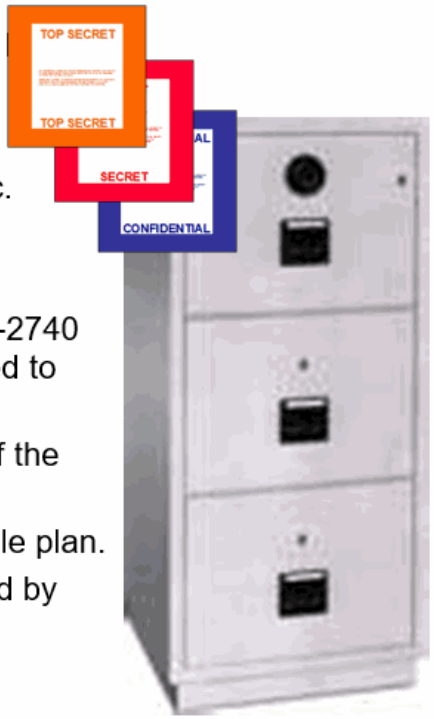
Pre-Publication Release

- ***Pre-Publication***
  - All government information must be submitted for a pre-publication security and policy review prior to release. Pre-publication review includes, but is not limited to:
    - Manuscripts, books, thesis
    - Conference papers, briefings
    - Articles, Biographies, speeches
    - Research and Scientific Papers
    - International Traffic in Arms Regulations technical Data
    - Congressional hearing statements
    - Reports to Congress
  - Coordinate with your local public affairs office or chain of command to facilitate the review of information.
- ***Who must submit material for public release?***
  - All current, former, and retired DON employees, contractors, and military service members (whether active or reserve) who have had access to DON information, facilities, or who signed a Non-Disclosure Agreement (NDA).
  - https://www.esd.whs.mil/Security-Review/PrePublication-and-Manuscripts/

Protection of DoD information is a lifelong responsibility. That responsibility does not end when an individual is no longer associated with the DON.

Storage and Destruction

- Information storage requirements vary based on the classification
  - **Top Secret** – See DoDM 5200.01 V3 enclosure 3, section 3, a.
  - **Secret** - See DoDM 5200.01 V3 enclosure 3, section 3, b.
  - **Confidential** - See DoDM 5200.01 V3 enclosure 3, section 3, c.
- A system of security checks will be employed using the SF 701 and SF 702.
- As required by the DoDM 5200.01 V3, Federal Specification FF-L-2740 or Federal Specification FF-P-110 combination locks will be utilized to secure classified information.
- Open Storage Areas will adhere to the Appendix to Enclosure 3 of the DoDM 5200.01 V3.
- Destroy classified information in accordance with your approved file plan.
- Only equipment listed on the Evaluated Products List (EPL) issued by NSA may be used to destroy classified information.
- Hold annual clean-out days to reduce holdings.



Proper storage and destruction minimizes the risk of Unauthorized Disclosure.

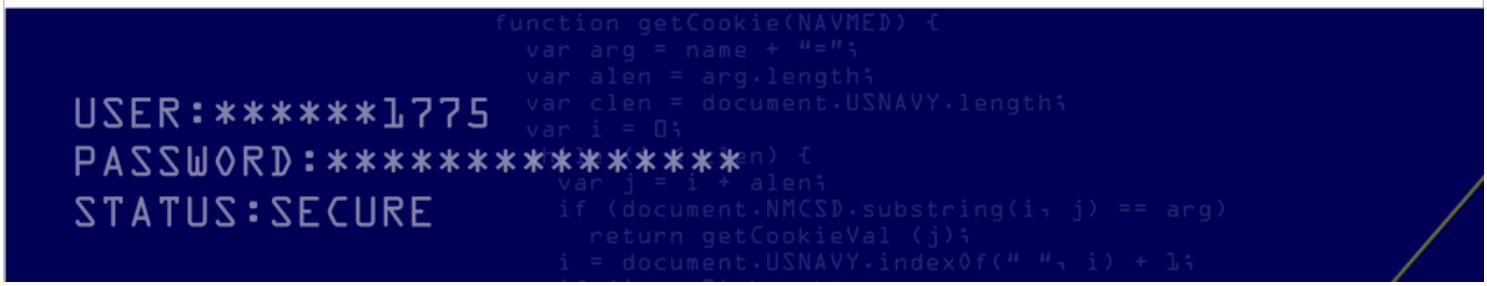
Transmission and Transportation

- Transmission requirements vary based on the classification level.
  - **Top Secret** - See DoDM 5200.01 V3 enclosure 4, section 3.
  - **Secret** - See DoDM 5200.01 V3 enclosure 3, section 4.
  - **Confidential** - See DoDM 5200.01 V3 enclosure 3, section 5.
- Classified information will only be transmitted to a foreign government as authorized by specific international agreement(s).
  - The absence of a "NOFORN" marking does not authorize the release of classified information to foreign governments.
- Classified information will only be transmitted on approved Information Technology systems/networks operating at the level commensurate with the data being transmitted.
  - Electronic transmission of classified information is preferred over physical transfer method.
- Classified material must be properly packaged for shipment.
- Minimize hand carrying of material to the greatest extent possible. See DoDM 5200.01 V3 Enclosure 4, section 12 for additional requirements.
- Consult with your ASM, GSSO or SSO prior to transporting any classified information.

Strict adherence to policy when transmitting and transportation classified material will mitigate the risk of Unauthorized Disclosure.

Cybersecurity Protocols

- Know your Information Assurance Manager (IAM).
- Complete Annual Information Systems Security Refresher Training.
- Use strong passwords/protect your password.
- Set your screensaver when you walk away from the computer.
- Report spillages of classified information on to lower classification systems to your IAM and SSO.
- Cross-domain transfers must be pre-approved and done in conjunction with the IAM or appointed systems member.



Conclusion

Security is an ALL HANDS effort.

Leadership must establish a strong *culture of security*

Information Security = National Security

If you ignore risk, you accept it

WE ARE ALL SECURITY PROFESSIONALS!

Information Security Standards Training

Questions?

Contact DUSN (I&S) for questions regarding these slides or DON security enterprise matters at dusnisinformationsecurity@us.navy.mil

Security Education Training and Awareness Resources

- All initial employee orientation briefings will contain the topics as required in DoDM 5200.01 V3 enclosure 5, section 3.
  - Sample briefing template: https://www.cdse.edu/Portals/124/Documents/jobaids/InitialOrientation_Customizable_Template_v2.pptx
- Access to Classified Information may only be granted to a person who, in carrying out his/her official duties or tasks, needs access to such information.
  - CDSE Video on Need-to-Know Principle: https://www.cdse.edu/Training/Security-Training-Videos/Personnel/Need-to-Know-Principle/
  - CDSE Video on Need-to-Know Principle (YouTube): https://youtu.be/ClsogcnYTac
  - Leaders will reinforce the understanding of Need-to-Know as part of Stand-down.
- There are multiple Security Education, Training and Awareness (SETA) courses on Navy E-Learning, USALearning, and the DCSA's Center for the Development of Security Excellence (CDSE) websites that Commanders may use to conduct refresher training
  - Navy E-Learning: https://learning.nel.navy.mil/ELIAASv2p/
  - CDSE: https://www.cdse.edu/catalog/elearning/IF141.html
  - USALearning: https://securityawareness.usalearning.gov/

Course Completion

Congratulations, you have completed this course. You must continue to the next page to record your training as complete and to view or print your certificate.