AR Division

UNAUTHORIZED DISCLOSURE TRAINING

AR Division

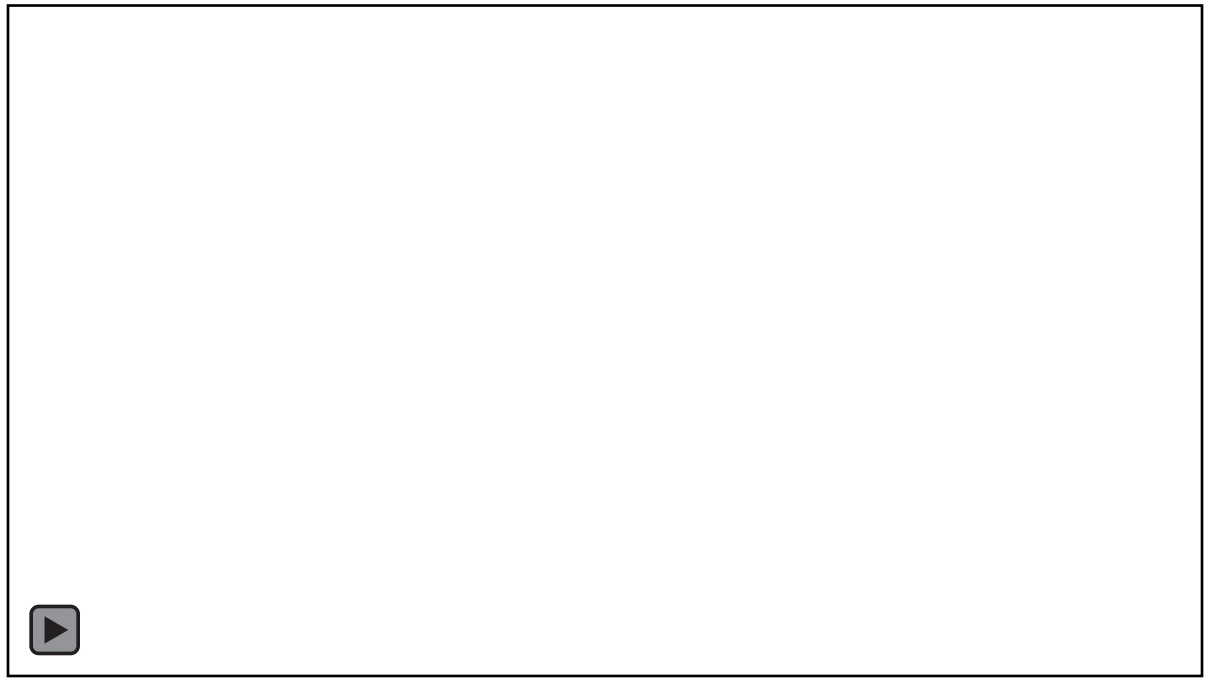
Overview

This training identifies and discusses employee's responsibilities for safeguarding classified information against unauthorized disclosures. This brief also outlines the criminal and administrative sanctions which can be imposed for an unauthorized disclosure. This training will focus on unauthorized disclosures to the media due to the significance of the damage these leaks have caused to national security.

AR Division

Attorney General/Director of National Intelligence Press Conference on National Security Leaks

"Click on the video to watch"



AR Division

Definitions

- ***Unauthorized Disclosure*** is the communication or physical transfer of classified information or controlled unclassified information (CUI) to an unauthorized recipient. These disclosures can be intentional or inadvertent, but either way, they can have serious repercussions.
  For example, media disclosure of classified information has significantly impaired U.S. capabilities against our hardest targets and done grave harm to national security.
- ***Espionage (spying)*** is the practice of spying or of using spies, typically by governments to obtain proprietary, political, and military information.

AR Division

Non-Disclosure Agreement (SF312)

- "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." This requirement is reiterated in the executive order on classified national security information. The SF 312 is a contractual agreement between the U.S. Government and you, a cleared employee, in which you agree never to disclose classified information to an unauthorized person. Its primary purpose is to inform you of:

  (1) the trust that is placed in you by providing you access to classified information;

  (2) your responsibilities to protect that information from unauthorized disclosure; and

  (3) the consequences that may result from your failure to meet those responsibilities. Additionally, by establishing the nature of this trust, your responsibilities, and the potential consequences of noncompliance in the context of a contractual agreement, if you violate that trust, the United States will be better able to prevent an unauthorized disclosure or to discipline you for such a disclosure by initiating a civil or administrative action.

AR Division

Misconceptions Regarding Unauthorized Disclosure

- If classified information appears in the news media, the internet, or other outlets in the public domain, the information is still considered classified until it is officially declassified:

  - Cleared employees are still legally bound not to view it.

  - Cleared personnel can be subject to sanctions if they seek out classified information in the public domain, acknowledge its accuracy or existence, or proliferate the information in any way.

  - If cleared employees do view it, then it must be reported as a data spill and the spill must be isolated and contained on the computer or other information system used to view it (e.g. BlackBerry, smartphone, tablet, etc.).

Misconceptions Regarding Unauthorized Disclosure - continue

- "Journalists' Privilege" does not allow reporters to protect their sources during grand jury proceedings.
- The Whistleblower Protection Act (PPD-19):
  - Protects employees from direct retaliation for acts of reporting protected disclosures.
  - Does not protect employees who unlawfully disclose classified information.
- The First Amendment does not guarantee protection to a cleared employee who discloses classified information unlawfully.
- Cleared employees are responsible for the protection of classified information or CUI, even after they are no longer employed by the government or by a cleared government contractor.

AR Division

Authorized Recipients of Classified Information and CUI

- Authorized recipients of classified information have:
  - Favorable determination of eligibility for access to classified information at the proper level.
  -"Need-to-know" for the classified information.
  - Signed SF-312, Classified Information Nondisclosure Agreement (NDA).
- Authorized recipients of CUI have:
  - "Need-to-know" for access to CUI.
  - Complied with other additional limitations and regulations, as applicable.
- Anyone who does not meet the above criteria is UNAUTHORIZED. This may include:
  - Media outlets.
  - The general public.
  - Coworkers and supervisors.
  - Foreign intelligence entities.

AR Division

Hackers Case

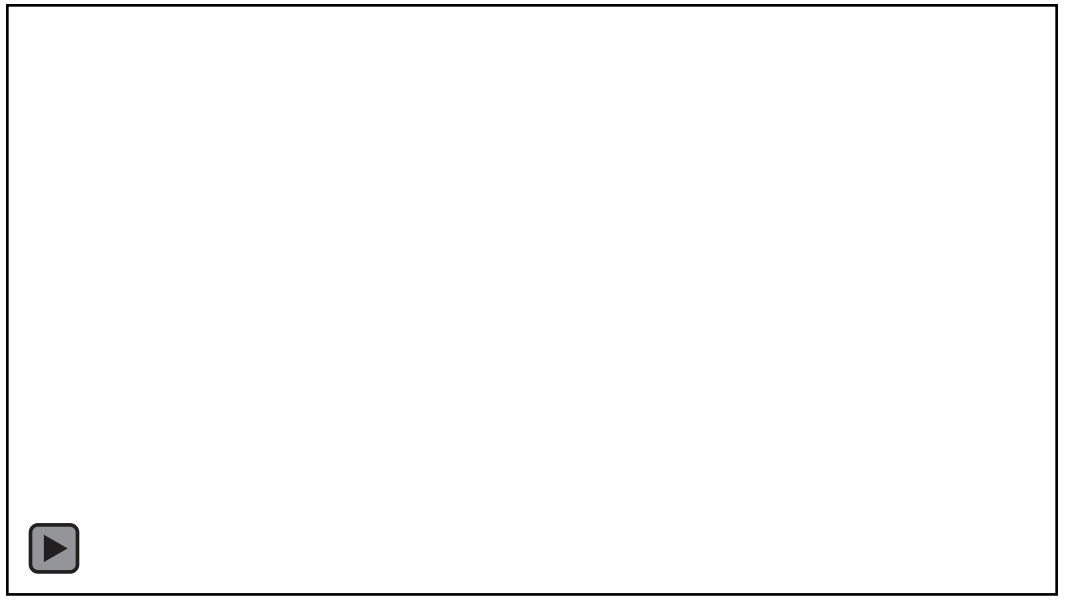
In April 2015, the Office of Personnel Management (OPM) was the subject of a cybersecurity incident (hacker attack) that affected its systems and data that compromised the personal information of current and former federal employees. An investigation conducted by Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) revealed that over 22.1 million people were affected by the breach. It was later discovered that the hack went deeper than initially believed and likely theft of detailed security-clearance related background information. On August 27, 2017, the FBI arrested a Chinese national suspected of helping to create the malware use in the breach.

AR Division

Whistleblower Protection Enhancement Act 2012

The Whistleblower Protection Enhancement Act of 2012 (WPEA) was signed into law by President Obama on November 27, 2012. The law strengthens the protection for federal employees who disclose evidence of waste, fraud, or abuse. Additionally, this law serves the Intelligence Community and personnel who are eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information.

"Click on the video to watch"



AR Division

Prepublication Review

- Within the DoD, all material undergoes prepublication review by the Defense Office of Prepublication and Security Review (DOPSR) to ensure it contains no classified information or CUI.
- Industry employees must consult their Facility Security Officer (FSO) and Government Contracting Activity (GCA) for guidance.
- Prepublication reviews are required before:
  - Sending any book, manuscript, or article to a publisher, editor, movie producer, game purveyor, or their respective support staffs.
  - Distributing any speech, briefing, article, or any content that will be publically available.
  - Releasing information to the public, even via Congress or the courts.
- Per DoDI 5230.29:
  - Prepublication review is **NOT** a declassification action.
  - Anyone submitting material for prepublication review must believe it is unclassified prior to submission.
  - Material submitted to DOPSR must first be coordinated and reviewed within the originating DoD Component.

Impacts of Unauthorized Disclosure

- Examples of damage caused by unauthorized disclosure include:
  - Damage to national security
  - Undermining of ongoing and planned U.S. operations
  - Potential loss of life
  - Damage to intelligence community sources and methods
  - Effect on international alliances
  - Financial costs
  - Reduces technological advantage over adversaries
  - Impact to foreign policy
  - Undermining of the public's confidence and trust
  - Benefit to adversaries wishing to harm U.S.

AR Division

Impacts of Unauthorized Disclosure – continued

Sanctions that may be applied if employees are responsible for unauthorized disclosure of classified information or CUI include:

- Uniform Code of Military Justice (UCMJ):
  - Loss of rank
  - Loss of pay
  - Dishonorable discharge
  - Incarceration

- Administrative sanctions:
  - Suspension without pay
  - Revocation of security clearance
  - Termination of employment
  - Loss of DoD contracts post-employment

- Civil litigation:
  - Loss of payments or royalties

- Criminal sanctions:
  - Incarceration
  - Fines
  - Loss of federal retirement benefits

AR Division

Responding to Unauthorized Disclosure

- Employees must:
  - Immediately protect the information.
  - Report unauthorized disclosure.

- If possible, immediately safeguard classified material.
  - Take personal possession of the classified material.
  - Secure classified material in an approved security container, other approved area or,
  - Provide the material to your Staff Agency/Activity Security Coordinator or HQMC Security Manager.

- For classified information suspected in the media or on the Internet:
  Do **NOT**:
  - View or download information.
  - Make any comment that confirms or verifies information.
  - Discuss information with anyone who does not have an appropriate security clearance and need-to-know.

AR Division

Responding to Unauthorized Disclosure – continued

Do:
- Provide point of contact for media inquiries:
- Refer all questions regarding media to Office Marine Corps Communications (OUSMC).

- When an Negligent Discharge of Classified Information (NDCI) or spill occurs, isolate and contain to:
  - Minimize damage (e.g. physically disconnect computer from the network).
  - Preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counterintelligence purposes (e.g. do not delete the information).
- Verify with the Original Classification Authority (OCA) that the information is classified. The OCA will ensure a damage assessment is conducted, if necessary.
- Refer to DoDM 5200.01, Vol. 4 and/or other regulations/policies as necessary for handling unauthorized disclosure or spills involving CUI.

AR Division

Report the Incident

Initial reporting:

- Report any of the following to your Security Manager (DoD) or FSO (industry):
  - Suspected or actual incidents of unauthorized disclosure
  - Attempts to solicit classified information
  - Violations of security regulations

- DoD:
  - Security Managers report incidents of unauthorized disclosure using the Security Incident Database (SID), the DoD-wide system for reporting serious security incidents.

- Industry:
  - FSOs report incidents of unauthorized disclosure, loss, compromise, or suspected compromise of classified information (including NDCI incidents) to their Industrial Security Representatives (IS Reps) who use the National Industrial Security System (NISS) to track security incidents and notify the Government Contracting Activity (GCA).

AR Division

Training Complete!

The next page is your completion certificate.
Complete it and send it to your Staff Agency/Activity Security Coordinator.

Certificate of Completion

I, _____ ,acknowledge that I have completed the HQMC Unauthorized Disclosure Training on

_____

DATE

_____

MEMBER'S SIGNATURE

_____

SECURITY COORDINATOR SIGNATURE