Mission Assurance for Senior Leaders:
Leaks and Spillage

Prevent leaks in your organization.
Know how to respond when they do occur.

Preventing Leaks and Spillage

A leak is the unauthorized disclosure of classified information to an unauthorized recipient. Data spillage is a specific kind of leak in which protected information moves from a higher classification or protection level to a lower one.

Security procedures to prevent leaks and spillage:

- Only release classified information to authorized recipients
    - Eligibility
    - "Need-to-know"
    - A signed SF-312, Classified Information Nondisclosure Agreement
- Ensure personnel follow procedures:
    - Apply appropriate classification markings and handling caveats
    - Be aware when unclassified information can be compiled
    - Remember which network you are on
    - Don't plug in devices to networks of different classification level

Consequences of Leaks and Spillage

When a leak or spill happens, a damage assessment is conducted to determine the effect on national security.

Damage assessments are conducted by:

- Original Classification Authority
- Subject matter experts
- Security officials, when appropriate

If involved in a leak or spill, personnel can face serious sanctions:

- Uniform Code of Military Justice prosecution
- Criminal prosecution
- Civil litigation
- Administrative sanctions

If criminal prosecution is warranted relating to a leak or spill from your organization, consult with DoD legal counsel.

Responding to Leaks and Spillage

Leaked classified or controlled information is *still* classified or controlled even if it has been compromised.

Classified information in the media:

- Do not download classified information viewed on the Internet
- Do not confirm or deny validity of information
- Only make statements if granted authority to do so

Remember, ***any*** comment by you will be seen as a statement by an official Government spokesperson.

As a senior leader, when responding to leaks and spillage, you should:

- Consult with security
- Isolate and contain spill
    - Minimize damage
    - Preserve evidence for damage assessment, risk assessment, law enforcement, or counterintelligence purposes
- Investigate incident
- Inform appropriate authorities internal and external to your organization:
    - Original Classification Authority (OCA)
    - Information owner/originator
    - Information Assurance Manager (IAM)/Information System Security Manager (ISSM)
    - Activity security manager
    - Responsible computer incident response center
    - Law enforcement
    - OUSD(I)

Report to OUSD(I):

- Espionage
- Disclosure in public media
- Significant harm to national security
- Most sensitive information or capabilities

OUSD(I):

- Determines investigative primacy when responsibility for an inquiry is unclear
- Reports incidents causing significant harm to national security or of great interest to the public to the U.S. Congress

Prevent leaks. Protect lives. Protect your mission.