How to Manage a Contamination Incident

Defense Security Service

Carolyn Shugart

Information Technology Specialist

Standards & Quality Branch

Objectives

- Define a compromise
- Define a contamination
- Describe the causes of a contamination
- Discuss preparing an ad hoc team
- Review steps for conducting an Administrative Inquiry
- Review reporting requirements
- Discuss cleanup considerations

What is a compromise?

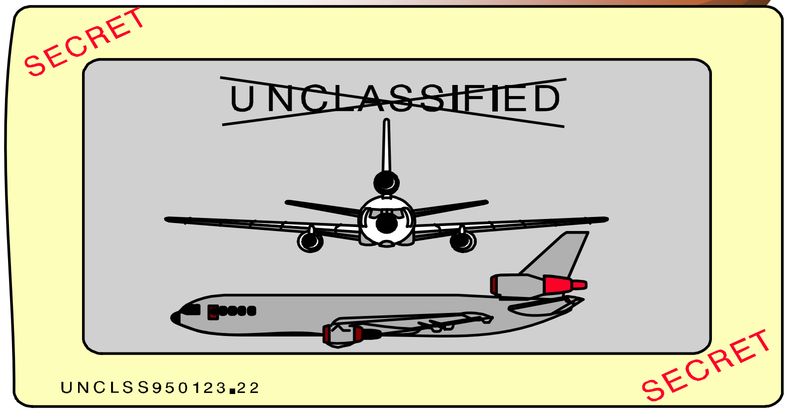
- **The disclosure of classified information to an unauthorized person**

What is a contamination?

- When classified information is processed on a non-accredited IS

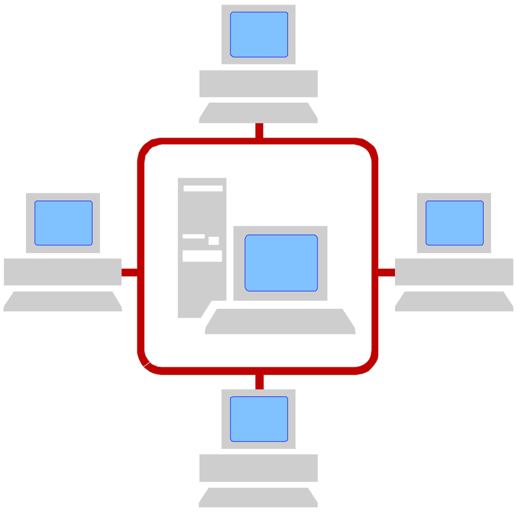
How does this happen?

- **Change in classification level**



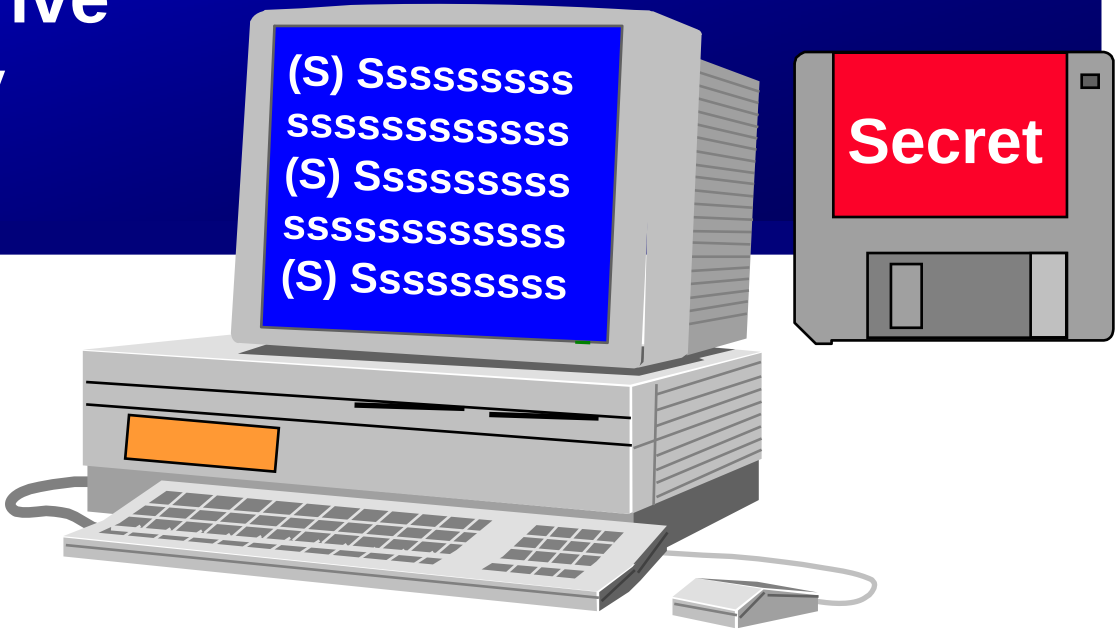
- **Unsecure transmission**

- **Accidental / intentional use of non-accredited equipment**

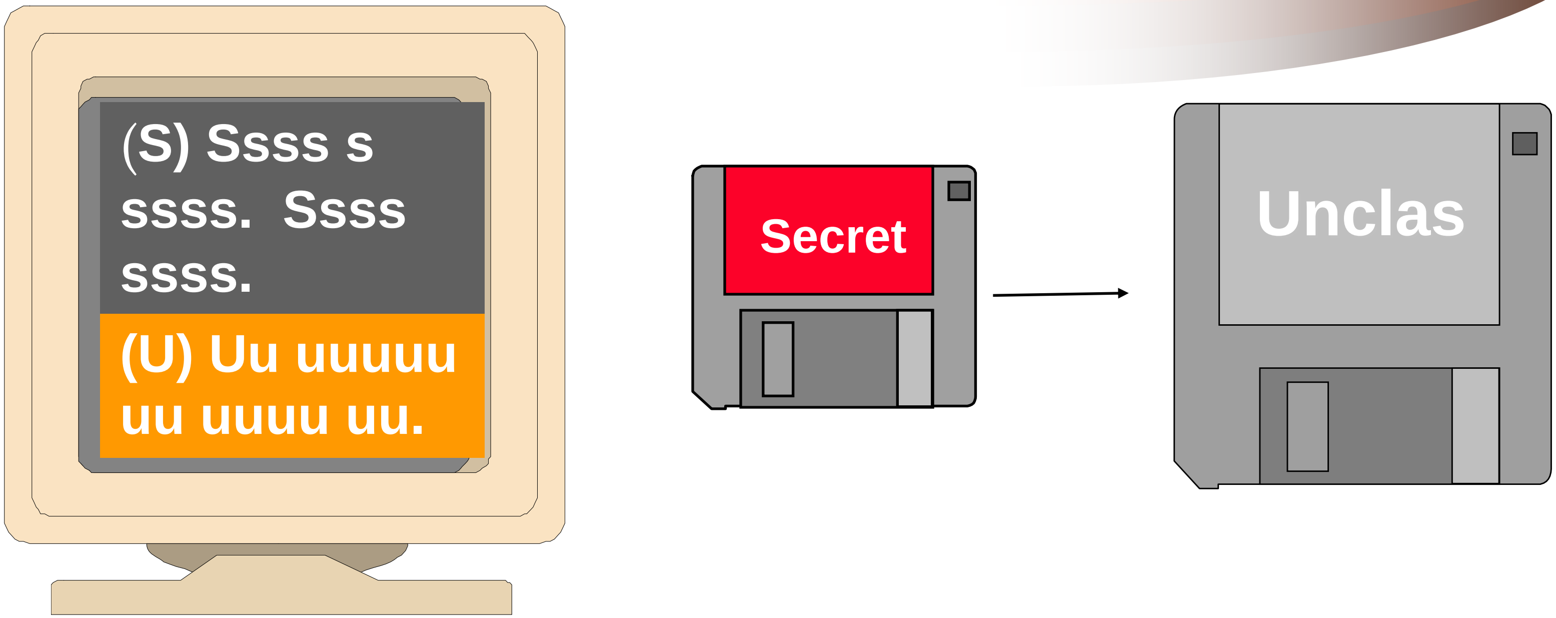


How does this happen?

- Unaccredited System with internal hard drive
- Cleared employee saves to floppy
- A temporary file created on internal hard drive then automatically deleted.



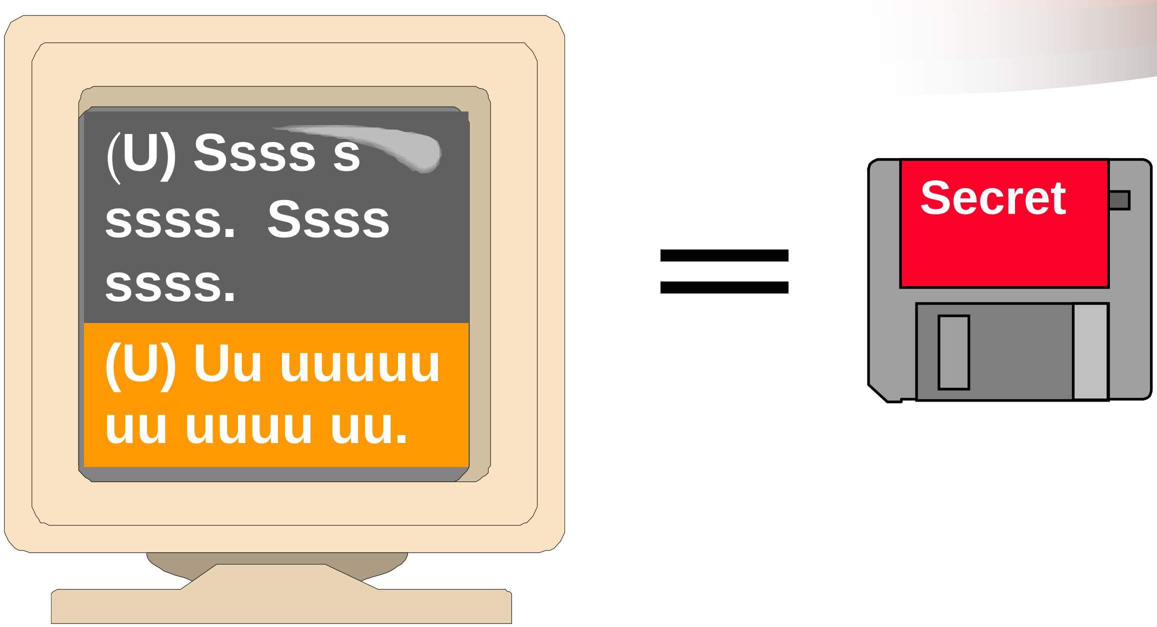
How does this happen?



1. “Track Changes” are hidden
2. Unclassified Extraction

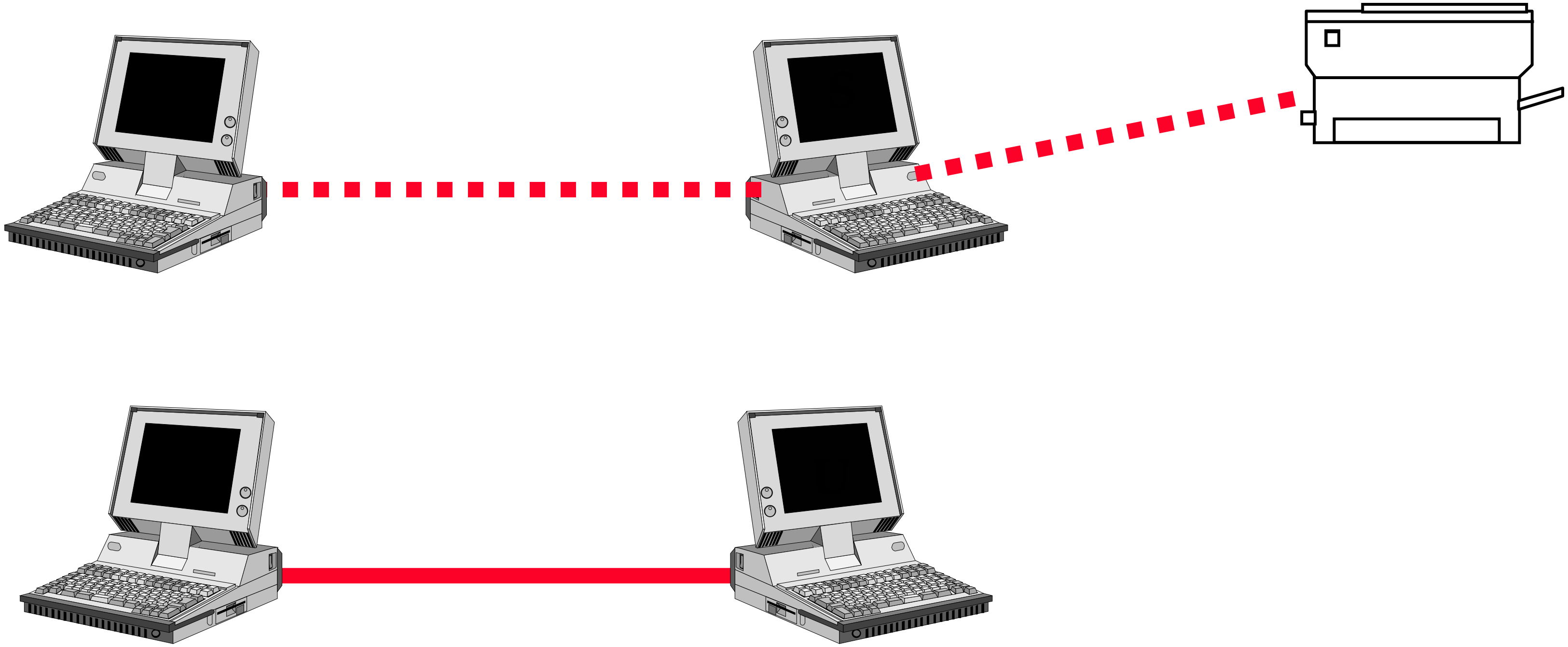
www.dss.mil/infoas/index.htm

How does this happen?



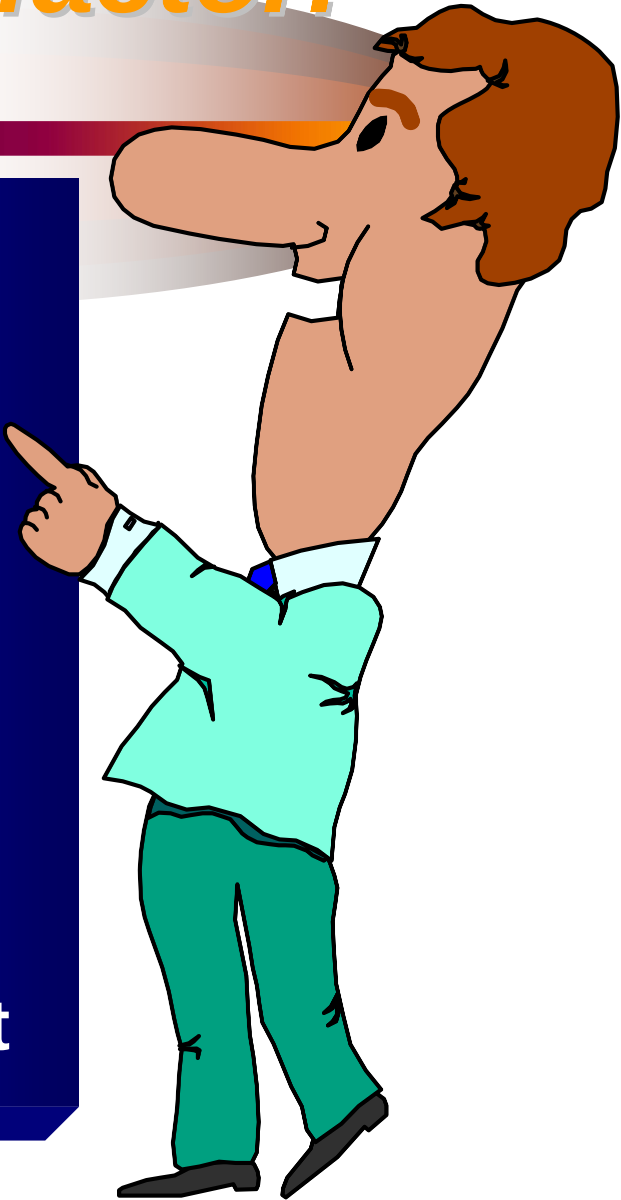
Compilation creates classified

How does this happen?



Attitudes can be a factor!

- People not following the rules
- Confusion
- Too busy to follow the rules
- Indifference
- It can’t happen here
- It cost too much
- Everyone else does it



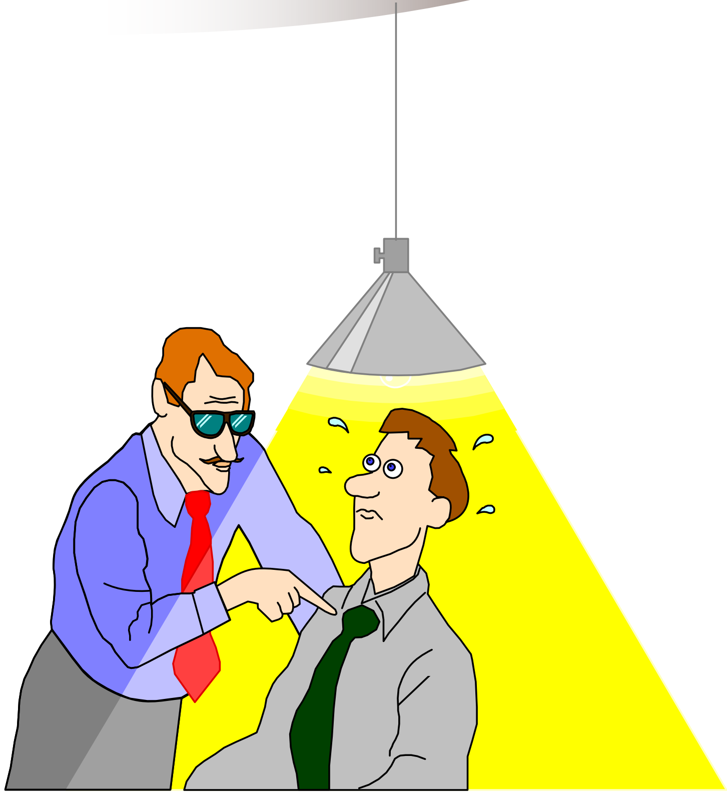
Before it happens, build an ad hoc team!

- No regular meetings
- SysAdmins proficient in each operating system
- SysAdmin proficient in email system
- Someone proficient in RAID drives
- Security Rep

RAID = Redundant Array of Independent Disks

Conducting an Administrative Inquiry!

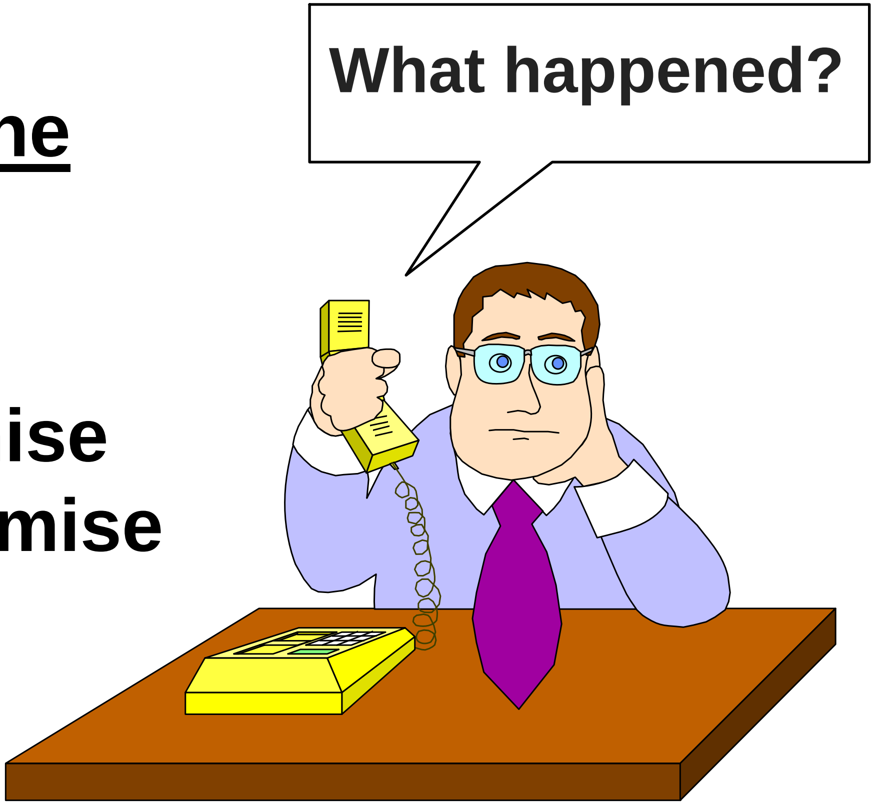
- Investigate the loss, compromise, or suspected compromise of classified information



NISPOM Para 1-303

Conduct a preliminary inquiry!

- Conduct *immediately*
- Identify W^5H, determine extent
- “Did a loss, compromise or suspected compromise occur?”



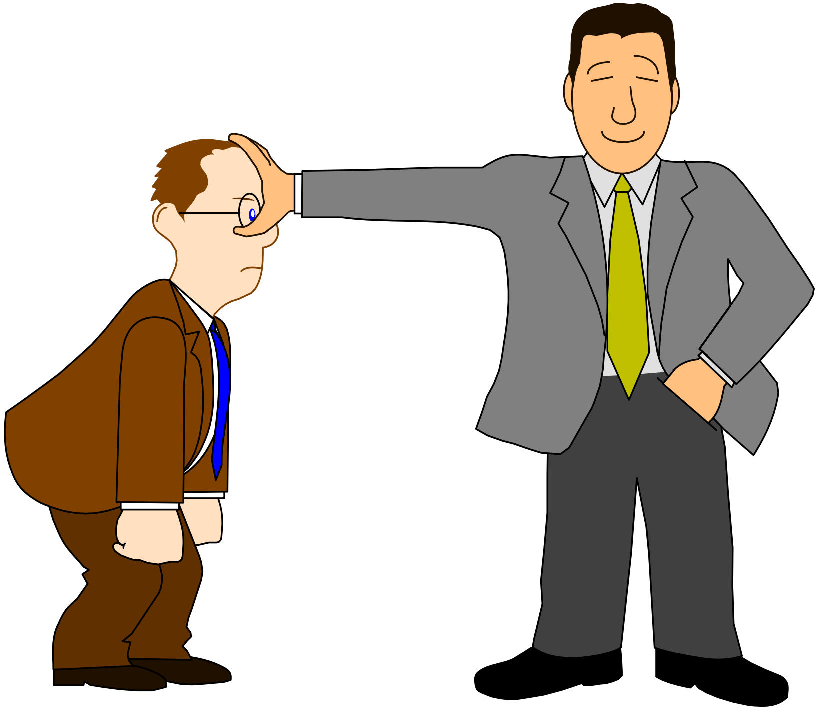
NISPOM Para 1-303a

Is there a loss, compromise, or suspected compromise?

- Loss: material can’t be located within a reasonable period of time
- Compromise: disclosure to unauthorized person(s)
- Suspected compromise: when disclosure can’t be reasonably precluded

Now what should be done?

- Assemble ad hoc team
- Physically isolate, protect all contaminated equipment
- Remove unauthorized people

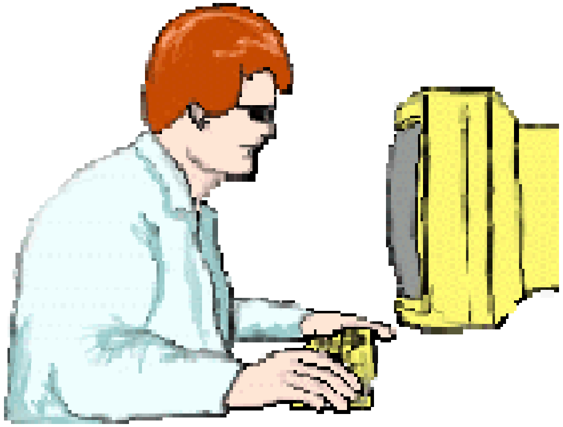


What should be done? (cont.)

- **Call your Defense Security Service (DSS) IS Rep and/or ISSP***
- **Contact your customer, the data owner**
- **DO NOT DELETE DATA YET!**

*** Information Systems Security Professional**

DO NOT DELETE THE FILE!!



“Would you take care of this for me!”

What will DSS do?

- Help you limit further systems from being contaminated.
- Work with you on sanitizing all infected systems.

What are important facts?

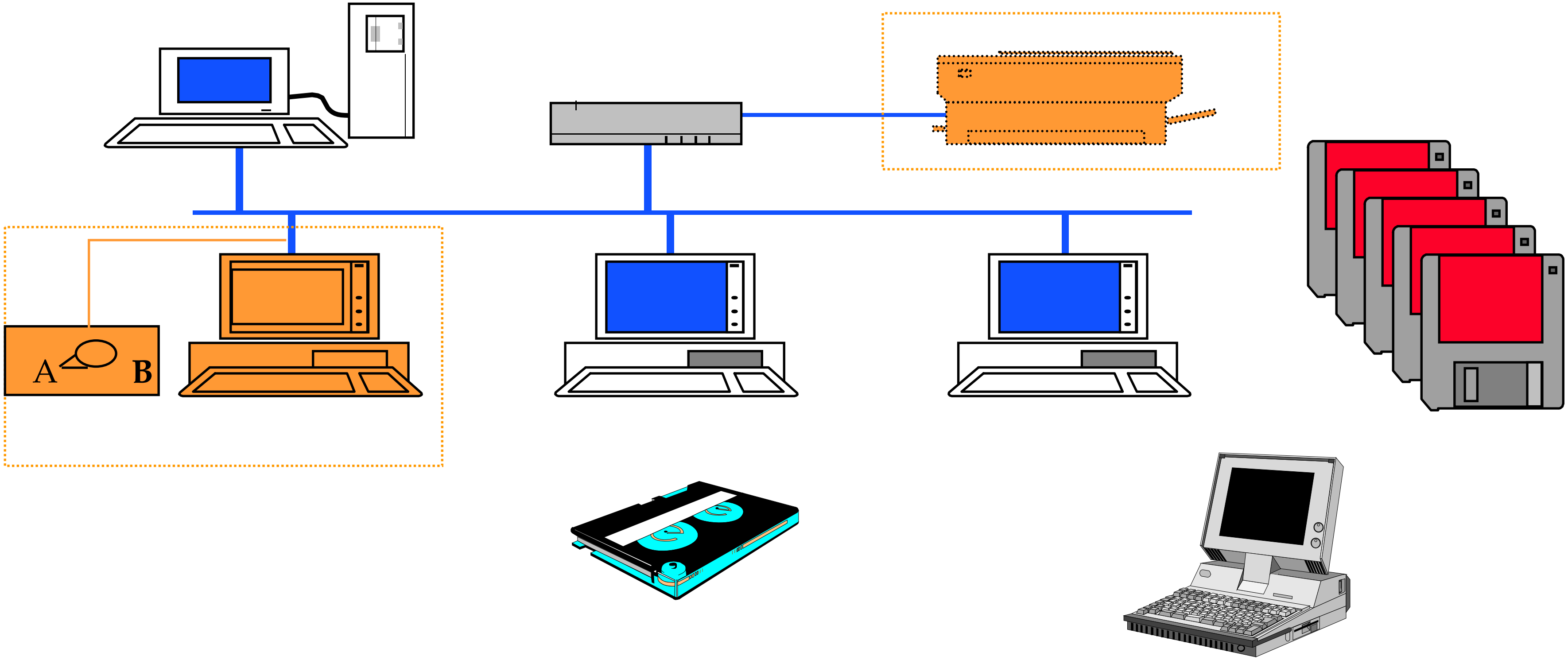
- What platforms and O/Ss are involved?
- Are there any remote dial-ins
- Are there any other network connections?
- At what locations was the file or e-mail received (e-mail servers) or placed?
- Was the data encrypted?
- Was the file deleted?
- Is there RAID technology involved?

What about an email server?

- What type of email system is involved?
- Is System Administrator cleared?
- Ensure areas where deleted files are retained are addressed, e.g., MS Exchange's deleted item recovery container).

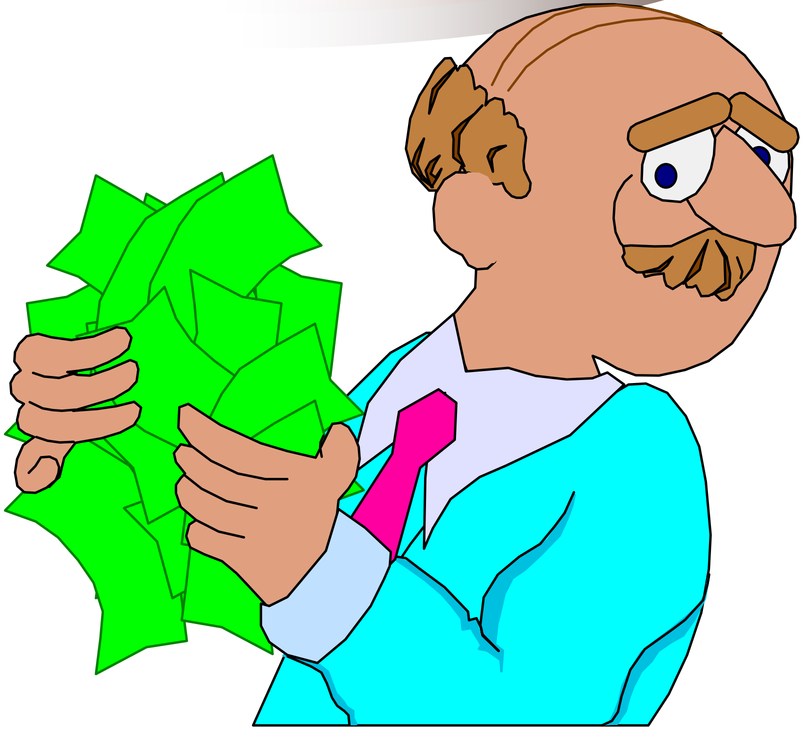
MS Exchange is discussed because of its widespread use. DSS does not endorse any products.

Forget any components?



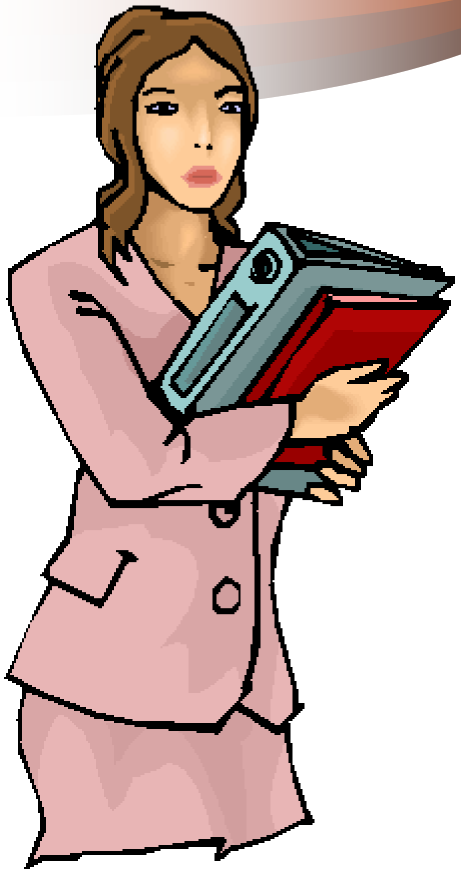
Follow through!

- Gather and review Audit Trails that are applicable
  - Paper
  - Electronic
- Interview all people known to be involved



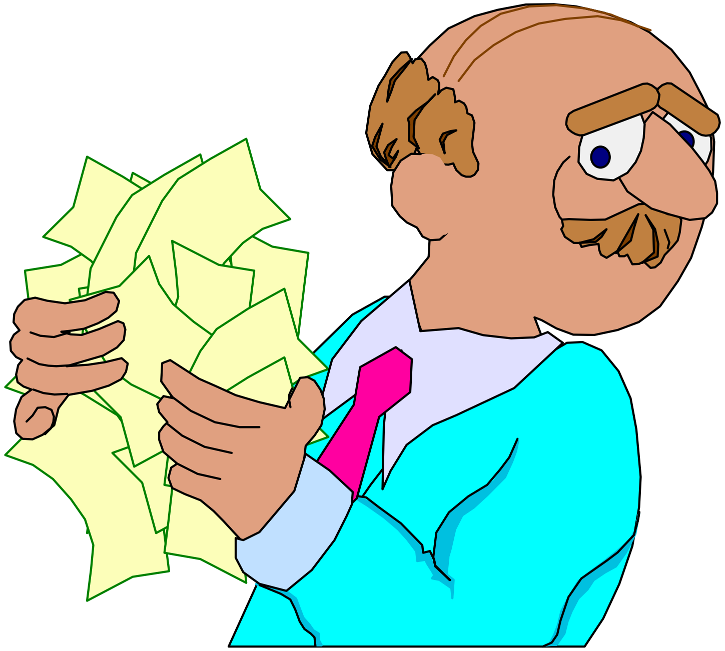
And finally…

- Write and submit the final report (Paragraph 1-303c, NISPOM)

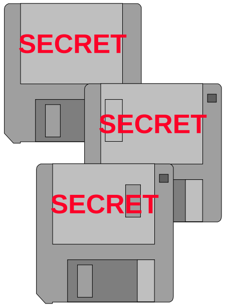


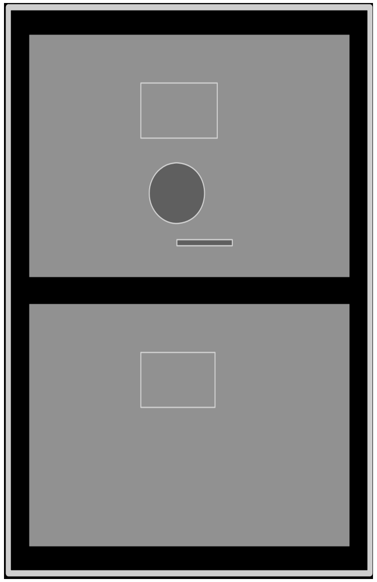
Follow available guidance!

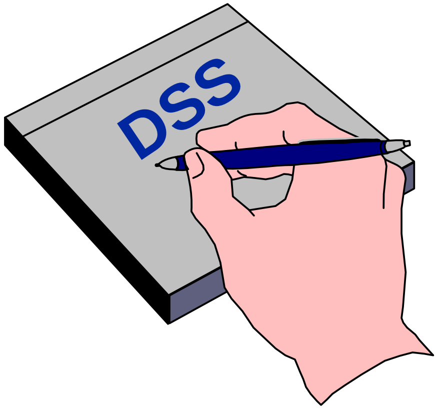
- **NISPOM AI Report Requirements (Paragraph 1-303)**
- **DSS Guidance for Conducting an AI**
- **Clearing and Sanitization Matrix**



And don’t forget to







- **Protect classified media**
- **Sanitize/clear the system components**
- **Write the report**

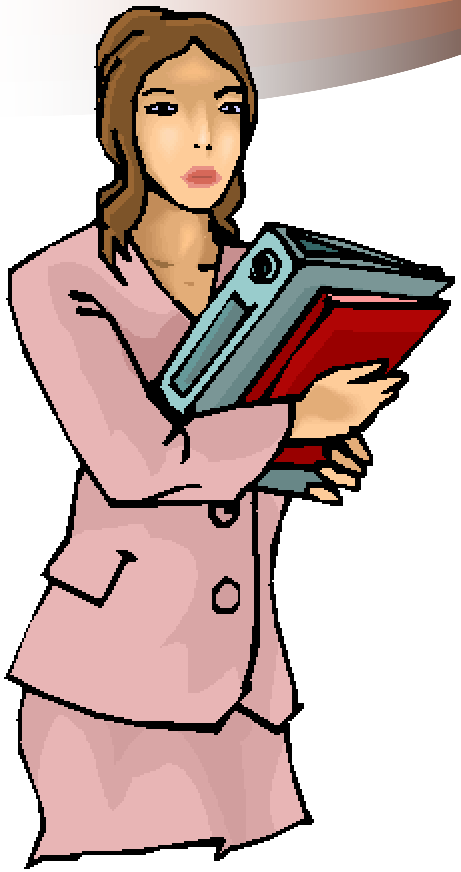
Report suspenses!

- Initial - “promptly submit” (72 hours)
- Final - investigation is complete (15 days)

NISPOM Para 1-303b,c

One last thing…

- Send details to government customer to include cleanup action
- Include hardware and operating system platforms
- Request they provide additional cleanup steps within 30 days



Summary

- What causes contaminations
- Possible cleanup considerations
- Reporting requirements

NISPOM Para 8-103b,c