

Initial Cyber Security Briefing

For New Hires, Visitors, and Contractors



Course 75.20

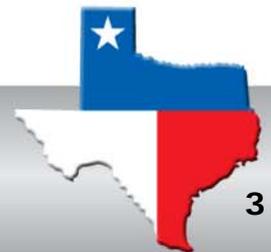
Chief Information Officer Division

Cyber Security Department



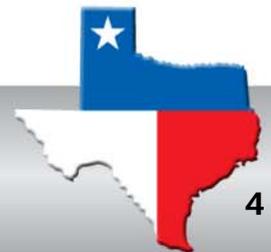
Enabling Objectives

- E01: Identify Who Must Comply with Cyber Security Requirements
- E02: Identify Primary Governing Document
- E03: Identify Cyber Security Concerns
- E04: Define Misuse of Computer Resources and the Consequences



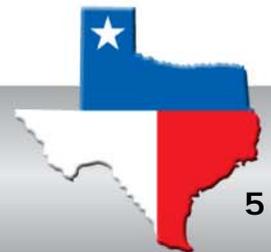
Enabling Objectives

- E05: Identify Items of Interest
- E06: Identify How to Get Help
- E07: Identify Purpose of Code of Conduct Statement



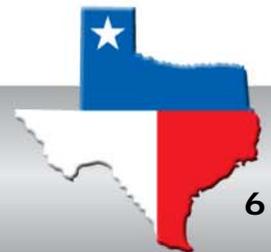
What is the role of Cyber Security

- **What is the role of Cyber Security?**
- **Why is this course important to you?**
- **Are you aware of any current cyber events?**
- **With whom do Cyber Security responsibilities lie?**



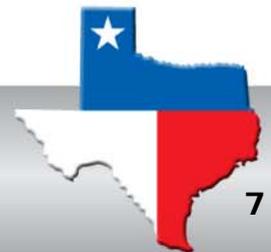
The Role of Cyber Security

- To assure that effective Cyber Security policies, procedures, and countermeasures are implemented in accordance with federal requirements and risk-based decisions, and guarantee the integrity, availability, and confidentiality of our information and systems
- In other words, to protect our nation's nuclear information



E01: Identify Who Must Comply with Cyber Security Requirements

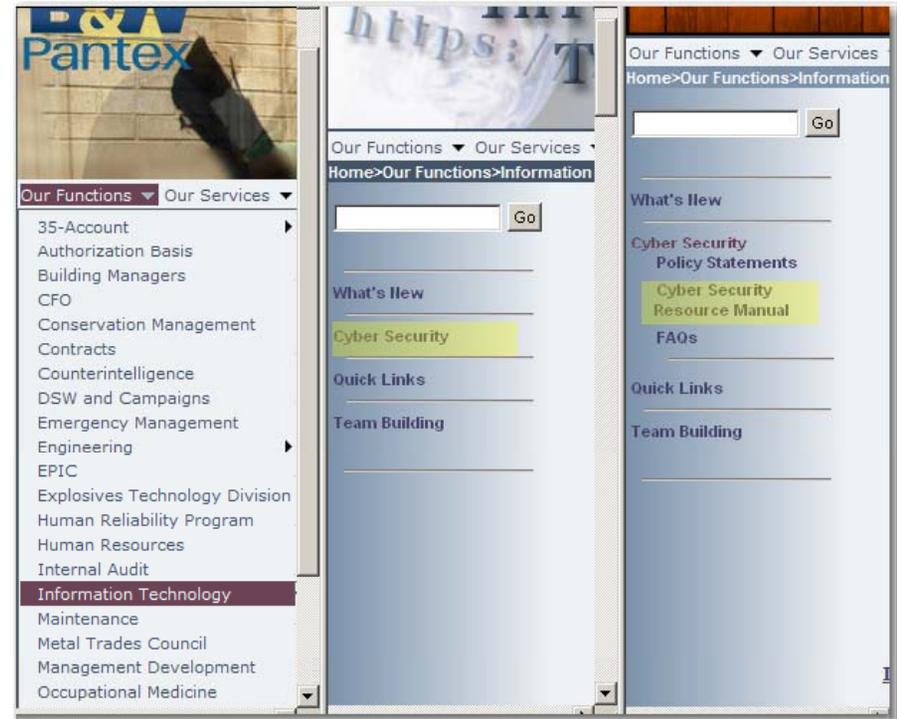
- **Everyone on Plant site**
 - Who will “use or have access to” Pantex computing resources
 - Must have some form of training before using such resources
- **If you will be onsite over 10 working days:**
 - Required to take [CBT 75.37](#) within three weeks of this briefing or your computer access will be suspended. You must work with your Division Training Officer to complete this training



Identify Primary Governing Document

The CSRM can be found on the:

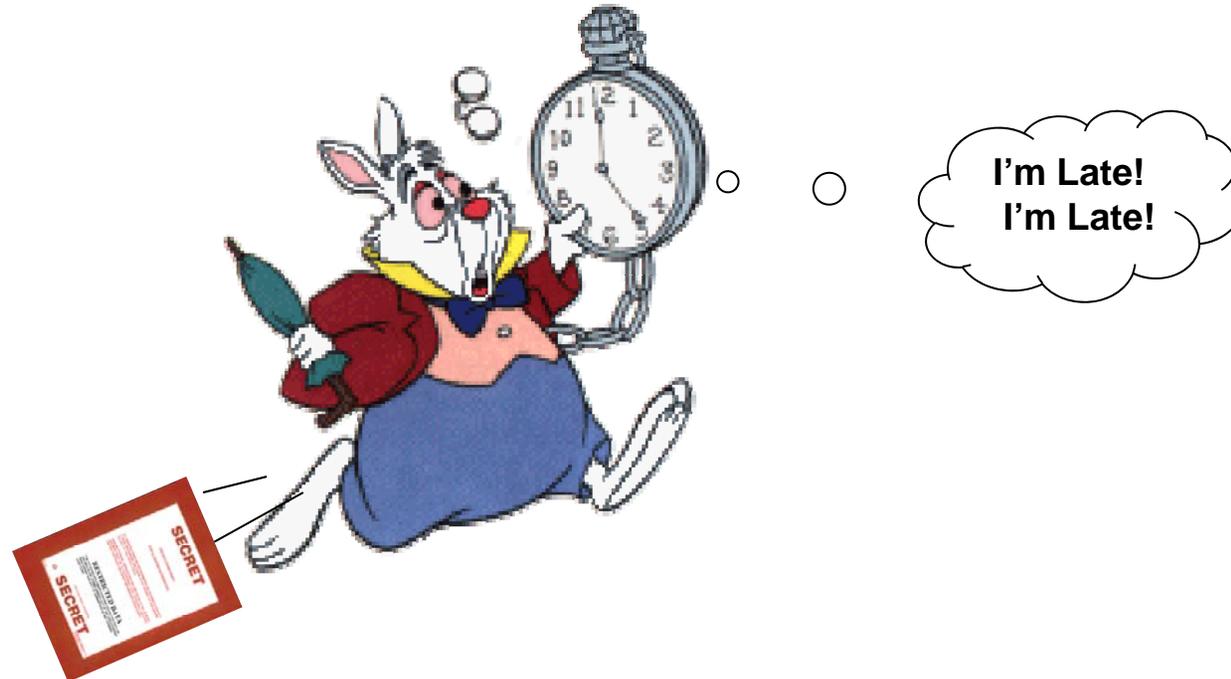
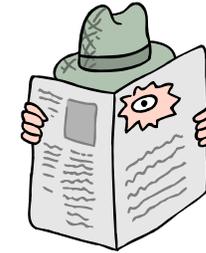
- **Cyber Security internal web page**
- **Universal Content Manager (UCM)**



E03: Identify Cyber Security Concerns

■ Insider Threat

- The “*deliberate*” insider or
- The “*accidental*” insider



Cyber Security Concerns

You can become an accidental insider if you:

- ◆ Are too busy, have a deadline to meet
- ◆ Don't lock your computer system
- ◆ Leave unprotected information on your desk
- ◆ Don't think the rules apply to you

Don't become part of the problem

Protection of computer resources and our nation's information depends on **YOU!**

Cyber Security Concerns

- **Phishing, Spear-phishing, and SPAM**
 - ◆ NEVER OPEN email from an unknown source
 - ◆ NEVER respond to requests for personal data
 - ◆ NEVER click on embedded links
 - ◆ Don't put your Pantex email out for "harvesting"
 - ◆ Send SPAM to SPAM@Pantex.com (see our web page for instructions)



Cyber Security Concerns

- **Personally Identifiable Information (PII)**
 - ◆ Never send it via email unless it is **encrypted** with an approved application (Entrust™ or PointSec™ or WinZip™ Pro)
 - ◆ BE CAREFUL about responding to emails with PII
 - Don't hit "Reply" without removing the PII



Cyber Security Concerns

Controlled Unclassified Information (CUI)

■ OOU and UCNI

- Official Use Only (OOU)
- Unclassified Controlled Nuclear Information (UCNI)



■ All require special protection

- Never send it via email unless it is **encrypted** with an approved application (Entrust™ or PointSec™, or WinZip™ Pro)

E04: Define Misuse of Computer Resources and the Consequences

- **Official business use only**
 - Exceptions:
 - ◆ Approved educational activities (after or before work hours)
 - ◆ Participation in Company-supported activities
 - United Way
 - Christmas Project
 - Employee Events Council
 - Consequences: Up to and including termination

Misuse of Computer Resources and the Consequences

- **You need to know**
Cyber Security monitors:

- Internal and external systems
 - Intruder attempts
 - Unauthorized use
 - Passwords that don't meet criteria
- Email transmissions
 - ◆ Classified information
 - ◆ Unencrypted CUI
 - ◆ Embedded or attached pictures



- **There is NO expectation of privacy**

Misuse of Computer Resources and the Consequences

■ Some issues that generate a Cyber Incident/Security Infraction

1. Compromise of passwords
 - ◆ Never write down a password
 - ◆ Never share a password
 - ◆ Classified and unclassified passwords must never be the same
2. Abuse or misuse of Internet access
3. Misuse of the email system
4. Contamination of unclassified system with classified data
5. Viewing/saving sexually explicit/suggestive material



Misuse of Computer Resources and the Consequences



If you know of or witness an incident, you **MUST** report it immediately to the Cyber Security Inquiry Official at extension **3818**

E05: Identify Items of Cyber Interest

Unapproved Items

The following personally owned articles are prohibited in the Security Areas (Property Protected, Limited, Protected, and Material Access Areas):

- Wireless keyboards
- Laptops
- Software of any type, including screensavers



Items of Cyber Interest

Approved Items – on **unclassified** computer systems only

- Music CDs/DVDs
- Personal thumb drives are approved for read access only
- IronKey thumb drives are the only thumb drives approved for read/write use



E06: Identify how to get help

- **Getting help with Cyber Security issues is easy!**
 - Call the Cyber Hotline, extension **7060**
 - Go to our Cyber Web Page (Our Functions / Information Technology / Cyber Security)
 - Dial a member of Cyber Security direct (See our web page)

E07: Identify Purpose of the Code of Conduct Statement

Code of Conduct Statement for Computer Users, PX-3115

Federal requirements state that all personnel must be trained in the general requirements for protection of our computing resources

Purpose of the Code of Conduct Statement

- **When you sign the PX-3115 you are confirming that you:**
 - Agree to comply with all rules and procedures for use of Pantex information resources
 - Will use the computer system for official business use only
 - Accept your responsibility for protecting government computing resources and information it processes

Things to Remember

- Protection of computer resources and our nation's information depends on **YOU!**
- There is no expectation for privacy
- Encrypt all outgoing Controlled Unclassified Information, including PII

Don't Forget: CBT 75.37 within three weeks of this briefing

Conclusion

You are responsible, but we are here to help.
Please ask before you act!

Questions and Answers!