

Initial Cyber Security Briefing

For New Hires, Visitors, and Contractors

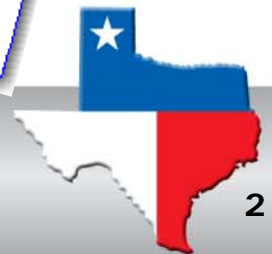
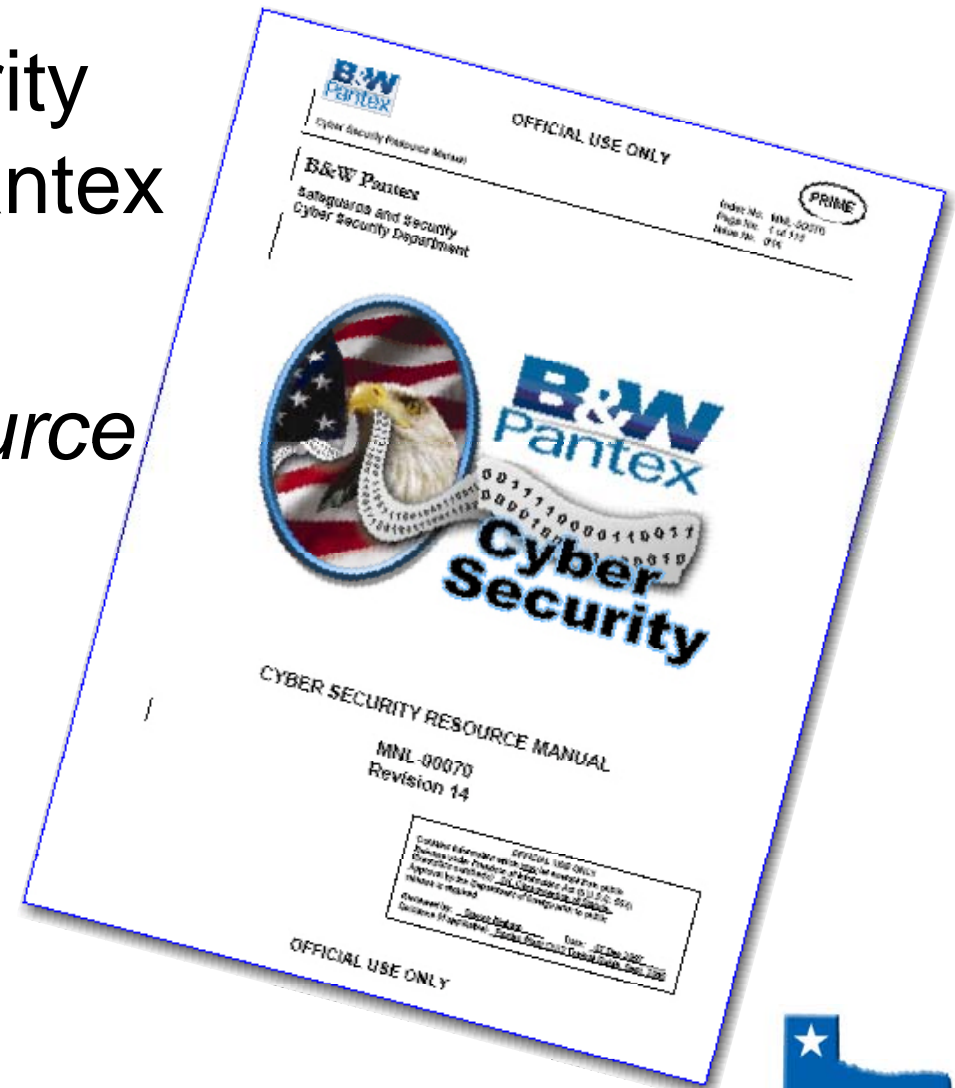


Course 75.20
Safeguards & Security
Cyber Security



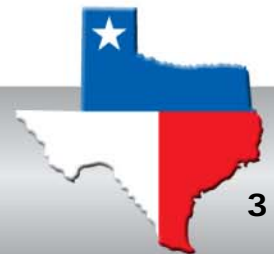
GOAL

Introduce cyber security requirements at Pantex as outlined in the *Cyber Security Resource Manual (MNL-00070)*.



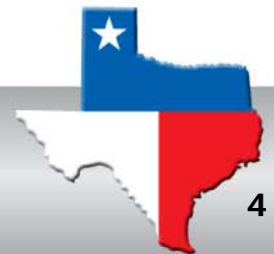
Enabling Objectives

- E01: Identify controlled media items
- E02: Identify primary governing document
- E03: Identify information resources
- E04: Identify who must comply with cyber security requirements



Enabling Objectives (Cont)

- E05: Define misuse of government computing resources and the consequences
- E06: Identify how to get help
- E07: Identify purpose of Code of Conduct Statement



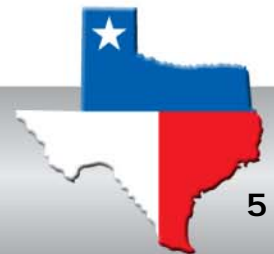
ISSM and Cyber Security

- **Define the Scope of Work**

- Cyber Security is a program to protect government information. For success, everyone here must actively participate in that mission.

- **Analyze the Risk**

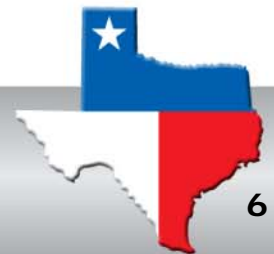
- Without conformance to the policies and procedures identified in this training, our systems, the information they process, and National Security are at risk of intrusion, accidental information release, or contamination of data.
- Foreign agents never rest in their attempts to uncover and steal the information that we work with.



ISSM Considerations

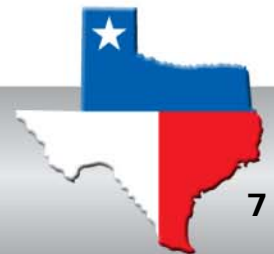
- **Develop & Implement Security Measures**
 - This briefing introduces the policies and procedures that implement information system security measures at Pantex Plant.

- **Perform Work within Measures and Controls**
 - All personnel are required to use Pantex computing systems within the controls established by MNL-00070, *Cyber Security Resource Manual (aka the CSRM)* and associated Work Instructions. If a question arises regarding safety or security of an operation, work must cease until the question is resolved.



ISSM Considerations

- **Provide Feedback and Continuous Improvement**
 - Your completion of the course evaluation provides the feedback that we need to improve it.
 - Suggestions are incorporated into the training at the next regular review cycle.
 - As new hazards and threats are identified, they are communicated to the Plant and incorporated into training.



E01: Identify Controlled Media Items

The following personal, company or government owned articles are controlled (prohibited in any area of the Plant, including Medical and the Cafeterias). **They *must* be left in personal vehicles.**

- Cell phones and cameras
- Voice recording capability

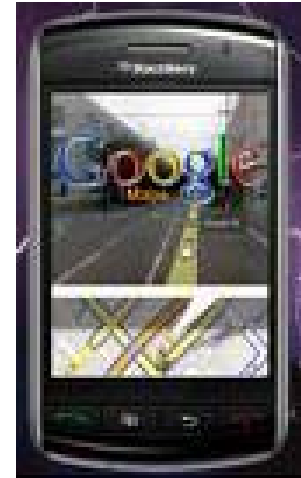


Controlled Media (continued)

These include:

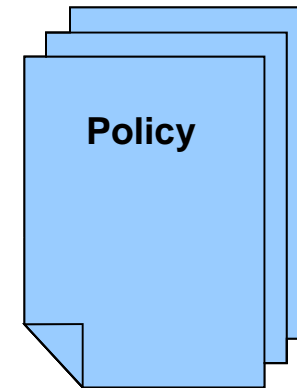
Portable Computing & Communication Devices (PCCDs) (formerly PEDs or PDAs, etc.)

- **Palm Pilot™, Pocket PC™, Blackberry™, etc.**
- MP3 devices
- Two-way pagers
- Wireless keyboards or networks
- Digital photo frames
- Recordable greeting cards
- Electronic book readers (Kindle™ etc.)



E02: Identify Primary Governing Document

- Cyber Security is
 - Policies and procedures
 - Practices
 - ◆ To protect computing resources & information processed



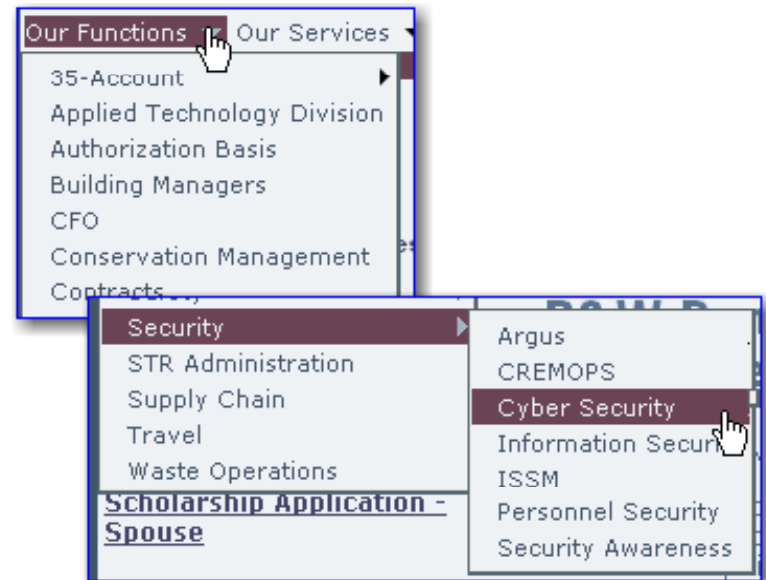
BUILDING WALK-THRU
CHECK LIST

Date: _____ Building: _____ ISSO: _____
Date: _____ Building: _____ ISSO: _____

No.	Description	"X"
1.	Classified system left unattended and unprotected? ** (Remember: a screen saver does not protect a classified system.)	
3.	Repository left unattended and unprotected? **	
4.	Illegal screen savers? (i.e. Spellman aquarium)	

Primary Governing Document

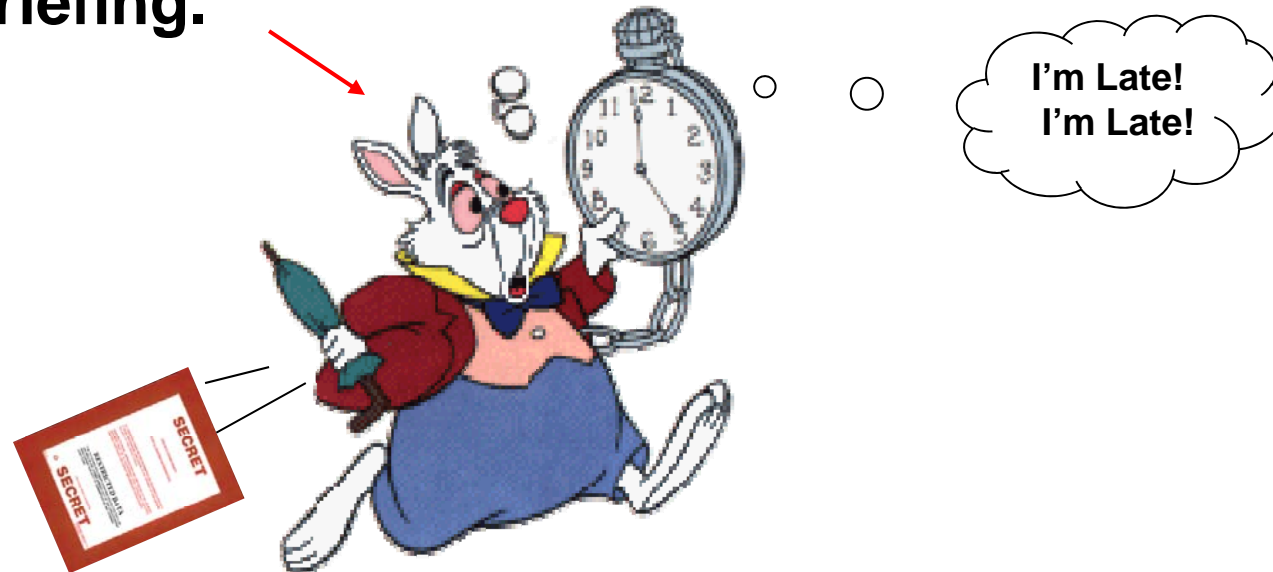
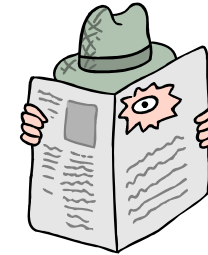
- **MNL-00070, the Cyber Security Resource Manual**
 - Work Instructions amplify processes
 - **CSRM is on the Cyber Security → internal web page**
 - Also in U.C.M. (Universal Content Manager)



What are we most concerned about?

■ Insider Threat

- The “*deliberate*” insider or
- The “*accidental*” insider.
 - ◆ This one is a focus for this briefing.



The Insider Threat



- **Phishing or Spear-phishing**
 - ◆ 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 the Cyber Technicians (see our web page for instructions)

The Insider Threat

- **Personally Identifiable Information (PII)**
 - ◆ Never send it via email unless **encrypted** with an approved application (Entrust™ or PointSec™ or WinZip™ Pro 12)
 - ◆ BE CAREFUL about responding to emails with PII
 - “Don’t hit “Reply” without removing PII”



The Insider Threat

- **OUO and UCNI**

- Official Use Only (OUO)
- Unclassified Controlled Nuclear Information (UCNI)
 - ◆ New term is SUI ([Sensitive Unclassified Information](#))



- **All require special protection**

- Never send it via email unless **encrypted** with an approved application (Entrust™ or PointSec™, or WinZip™ Pro 12)
- CAREFUL about combining documents—you could create a classified document.

E03: Identify Information Resources

- Information Resources
 - Hardware & Software
 - Database Files
 - E-mail & Internet
 - Special purpose systems and applications
 - **YOU!** If you
 - ◆ Are too busy, have a deadline to meet
 - ◆ Don't think the rules apply to you
 - ◆ Just not feeling well, etc.
 - You could become part of the problem

E04: 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 any computer access will be suspended without notice.

E05: Define Misuse & Consequences

- **Official business use only**
 - Exceptions:
 - ◆ Approved educational activities
 - ◆ Participation in Company-supported activities
 - United Way, Christmas Project, Employee Events Council
- Consequences: Up to and including discharge
- ***“Zero Tolerance”*** policy

E05: Define Misuse & Consequences

- **You need to know**

- **Cyber Security routinely monitors**

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

E05: Define Misuse & Consequences

- **Some issues that generate a Cyber Incident**
 1. Compromise of passwords
 - ◆ Never write down a password
 - ◆ Never share a password
 - ◆ Never create your password for classified systems
 2. Abuse or misuse of Internet access
 3. Misuse of the email system
 4. Leaving classified unattended
 5. Contamination of unclassified system with classified data
 6. Viewing/saving sexually explicit/suggestive material

E05: Define Misuse & Consequences



The last three issues **MUST** be reported immediately to the Cyber Security Inquiry Official at extension **3818**.

E06: Identify how to get help

- **Getting help with Cyber Security issues is easy!**

1. Call the Cyber Hotline, ext. **7060**.
2. Go to our Cyber Web Page (Our Functions / Security / Cyber Security).
3. Dial a member of Cyber direct. (See our web page.)

E07: Identify Purpose of Code of Conduct Statement

- Federal requirements state that we must train all personnel in the general requirements for protection of our computing resources.
- When you sign the PX-3115, Code of Conduct Statement for Computer Users, you are confirming in writing that you have received initial training in the form of this briefing.

E07: Code of Conduct Statement

- **You are also confirming that you**
 - Agree to comply with all rules and procedures for use of such information resources, and
 - Accept your responsibility for protecting government computing resources and information.

You are responsible, but we are here to help you,
so please ask before you act!

Don't Forget: **75.37** within three weeks.