



# Princeton Plasma Physics Laboratory

Cyber Security Overview  
Steve Baumgartner  
CIO & Computer Division Head  
July 2008



# Cyber Security at PPPL

## Cyber Security Strategic Goal:

***“Protect DOE information and information systems to ensure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats.”***

DOE Cyber Security Strategic Plan – February 12, 2007



# Cyber Security at PPPL

- Systems are assessed according to the National Institute of Standards & Technology (NIST) guidance and Federal Information Processing Standards (FIPS) for the likelihood of exploitation and its impact on PPPL.
  - Systems with greater risk or impact on PPPL's mission such as NSTX Controls or systems containing PII (Personally Identifiable Information) require the implementation of additional controls.
  - All Office of Science laboratories are required to follow NIST Special Publication 800-53 Rev1 "Recommended Security Controls for Federal Information Systems".



# Cyber Security at PPPL

## **A robust Cyber Security program consists of multiple layers of defense:**

- Strong perimeter.
- Best Practices for Authentication Techniques.
- Controlled Authorization to services and systems .
- Configuration Management and patching.
- Emphasize training of employees and administrators.
- Extensive Logging and Alerts.
- Contingency Planning with Backups and Recovery.
- Physical Protection.
- Continuous monitoring, assessment and improvement.



# Cyber Security Consists of Layered Defenses

- Strong perimeter firewall and access rules.
  - “default deny” mode permits only “whitelisted” services versus “blacklisting” known threats.
  - All remote access requires 2-factor authentication.
  - Web-based Virtual Private Network (VPN) utilized for secure access and encryption.
- Network Registration is required for all networked devices.
  - Wired and wireless “visitors” network is separated from internal PPPL network.
  - Network is segregated into over 20 virtual local area networks (VLANs).
    - NSTX Controls and Diagnostics are on segregated VLANs with additional internal Firewall access controls.
  - Inter-VLAN traffic is controlled via dual internal firewalls.



# Cyber Security Consists of Layered Defenses

- Authentication is controlled through Windows Active Directory (Windows, Macs, Linux, Unix)
  - Access to NSTX Control systems requires approval of the Branch Head of Instrumentation & Controls.
  - All network passwords changed every 6 months.
  - Require strong password content with special characters, numerics and upper/lower case letters.
- Security updates and configurations are performed on all servers and workstations:
  - Windows Group Policy and Windows Software Update Server.
  - Apple Remote Desktop and Mac Domain
  - Up2date on Linux systems
  - McAfee Policy & Remediation Manager deployed to audit compliance.
  - NISSUS vulnerability scans are conducted daily, weekly and monthly or as required depending on the system.



# Cyber Security Consists of Layered Defenses

- Three levels of anti-virus protection are deployed throughout the laboratory:
  - Proofpoint Spam filter provides anti-virus and spam filtering at the gateway.
    - ~85% of inbound email is removed as spam.
  - Corporate Symantec anti-virus on the Exchange server processes all inbound email prior to delivery.
  - Symantec anti-virus is loaded and updated daily on all desktops.
- Employees are a significant line of defense but are also a system's greatest risk.
  - Annual Cyber Security Awareness Training is required for all employees.
    - Special emphasis on social engineering and “phishing” attacks.
  - System Administrators are required to receive professional skills training biennially.
  - Annual training required for incident response team.



# Cyber Security Consists of Layered Defenses

- Backup and Recovery
  - All systems, including NSTX, use Veritas Netbackup
  - NSTX Systems are backed up using a combination disk to disk and disk to tape strategies.
  - All servers and NSTX data are backed up daily, weekly and monthly.
    - Two months duplicates are stored off-site > 75 miles.
  - User desktops backed up daily, weekly and semi-annually or on demand.
- Physical Security
  - NSTX Control systems are located in access controlled areas.
  - Network switches and hubs are secured by key or card access.
  - All NSTX data is stored on the Storage Area Network located in the PPLCC
    - Card access controlled
    - Temperature & Humidity controls
    - CO<sub>2</sub> under the floor for fire suppression
    - Uninterrupted Power Supply (UPS) to avoid power loss or power fluctuations
    - 24 by 7 monitoring by Site Protection



# Continuous Monitoring

- Certification and Accreditation process performed every 3 years.
  - Completed in June 2007
  - Package includes: Threat Analysis; Cyber Security Program Plan; Risk Assessment; and Contingency Planning.
  - Security Testing & Evaluation performed by OnPoint Consulting.
- Self-Assessment in years between C&A process.
  - QA Audit of Cyber completed in 2008
- External Assessments:
  - Safeguards and Security Audits every 2 years
  - Health, Safety and Security audit completed in June 2008
    - Technical team was “shut out” for the first time ever.
    - Excellent Configuration Management and patching practices.



# Current Plans and Wrap Up

- Upgrade our current Intrusion Detection System (IDS)
- Replacement of the perimeter Firewall which is now over 4 years old.
- Working with Princeton University and ESnet, increase our Wide Area Network (WAN) to 10 Gb capability.
- Augment our current Network Access Control (NAC) system to include end-point inspection and Intrusion Prevention.

*At PPPL we strive to provide sufficient computer and network security to protect our systems and data while minimizing its detrimental effects on science and user productivity.*