

SLAC Computer Security Program May 6, 2009

(Very) Brief Overview for our new members of
Requirements
Program Structure
Sec Team Activities



Cyber Security ... Not just a best practice

- Required in SLAC contract
 - » A goal in the Contract Performance Evaluation and Measurement Plan (PEMP)

- Contract Requirements
 - » Cyber Security Order 205.1A→
 - Office of Science PCSP →
 - “a long list of legislation, NIST documents, and OMB memos that are incorporated into the PCSP (and hence into O205.1A)” ->
 - SLAC CSPP ->
 - Certification & Accreditation ->
 - = Authority to Operate from DAA (Paul Golan)

Enclaves

- Systems grouped into 9 accreditation boundaries grouping like systems (e.g. similar management, use, risk)
 - » EPN, Business Services, Infrastructure, Research, Visitor, MCC, PCDS, SSRL, and Collaboration
- Enclaves inherit common controls
 - » Any additional or deviation from common controls is documented
- Enclave owner responsible for assuring that the controls are documented, in place, and functioning properly

Other requirements sources

- Orders in Contract
 - » O 142.3 Unclassified Foreign Visits and Assignments
 - » O 200.1 Information Management Program
 - » O 471.3 Identifying and Protecting Official Use Only Information
 - » O 475.1 Counter Intelligence
- FISMA – Federal Information Security Management Act of 2002
 - » NIST SP 800 series
 - 800-53/53A Recommended Security Controls for Federal Information Systems
 - 800-37 Certification and Accreditation

Reporting and Data calls

- Data calls from DOE
 - » Quarterly FISMA Report
 - » Quarterly POA&M Report
 - » Quarterly Privacy Report
 - » Quarterly Cyber Security Report Card
 - » OMB Compliance Data calls (various, e.g. FDCC, DNSSEC)
- SLAC PEMP
 - » Quarterly Update
 - » Mid-Year/Year Status
- DOE CIRC, SSO, CI, IG
 - » Cyber Incidents
 - » Fraud/Waste/Abuse
 - » Counter Intelligence

Collaborations

- NLCIO
- DOE NSM (Network Security Monitoring)
- Federated Model for Intrusion Prevention

Operations

- Cyber security is a line management responsibility
- Some specific Team Activities
 - » Vulnerability Management/Risk Assessment
 - » Intrusion Analysis and Forensics
 - » Awareness and Training
 - » Intrusion Detection
 - » Compliance