



PennState

Institute for CyberScience

The Role of a System Security Plan (SSP)

Ryan Gilmore

ICS-ACI System Integration Lead



Defining an SSP

- ◆ A System Security Plan (SSP) essentially describes the security controls of the system and what state they are in
- ◆ Elements of the SSP:
 - ◆ Security POCs and roles for an organization
 - ◆ Requirements
 - ◆ Technical implementation of stated requirements
 - ◆ Current, Future State
 - ◆ Defined security boundary



The Benefit : Meeting Compliance Objectives

- ◆ Assessment of the requirements for applicability
 - ◆ Requirement mapping to test cases
- ◆ Determined which controls are common among multiple stakeholders such as the Data Center
- ◆ Demonstrating Compliance vs. “Saying” Compliance



Challenges and Considerations

- ◆ Provide a “Secure” environment while being as transparent as possible
- ◆ Communication and coordination between multiple organizations within the University
- ◆ The openness and diversity of research



Key Decisions

- ◆ Identify a template to use
 - ◆ Consider existing templates
 - ◆ Is anyone else going to rely on the SSP?
- ◆ Define what belongs in the SSP and what does **NOT**:
 - ◆ Process Management
 - ◆ Test Cases



Conclusions and Lessons Learned

- ◆ Required by NIST 800-171
- ◆ Intended Audience
- ◆ Identify common controls
- ◆ What certifications and/or ATOs are needed
- ◆ Responsibility for maintaining

