PEARC18:
HPC security and compliance workshop
Agenda

Date: Tuesday July 24, 2018
Location: Dusquesne room
Wyndham Grand Pittsburgh Downtown

Time: 10:30 am – 5:00 pm
Organizers: Erik Deumens deumens@ufl.edu and Joe Gridley jdg284@psu.edu

10:30 – 10:40 Opening remarks and plan of the workshop

Joe Gridley and Erik Deumens

10:30 -12:00 Business process and lifecycle of compliance for research

10:40 – 11:00	Greg Madden, gem19@psu.edu, Pennsylvania State University	Intra-Institutional Partnerships for Research Data Security and Compliance
11:00 – 11:20	Preston Smith, psmith@purdue.edu Purdue	Maturing REED from a Service to a Model
11:20 – 12:00		Discussion

12:00 – 13:30 Networking lunch

13:30 – 14:30 Writing a system security plan

13:30 – 13:50	Ryan Gilmore, reg159@psu.edu Institute for Cyberscience/PSU	The role of the System Security Plan
13:50 – 14:10	Mike Warfe, jmw22@case.edu Case Western Reserve University	You want me to do what? Musings on writing a system security plan with labs.
14:10 – 14:30	Andrew Spragg, ags5008@arl.psu.edu Applied Research Lab/PSU	Strategic decisions in planning your SSP

14:30 – 15:00 Controls: technical exploration and planning

14:30 – 14:45	Trey Breckenridge, trey@hpc.msstate.edu Mississippi State University	Assured Compliance through Information Security Continuous Monitoring
14:45 – 15:00	Maureen Dougherty, mdougher@usc.edu University Southern California	Building a Secure Data Environment

15:00 – 15:30 Break

15:30 – 16:30 Technical discussion

Families: access AC, audit AU, configuration CM, identification IA, physical PE, system and communication SC, system and information integrity SI	**Discussion leaders:** Neil Bright, ncbright@gatech.edu Erik Deumens Joe Gridley

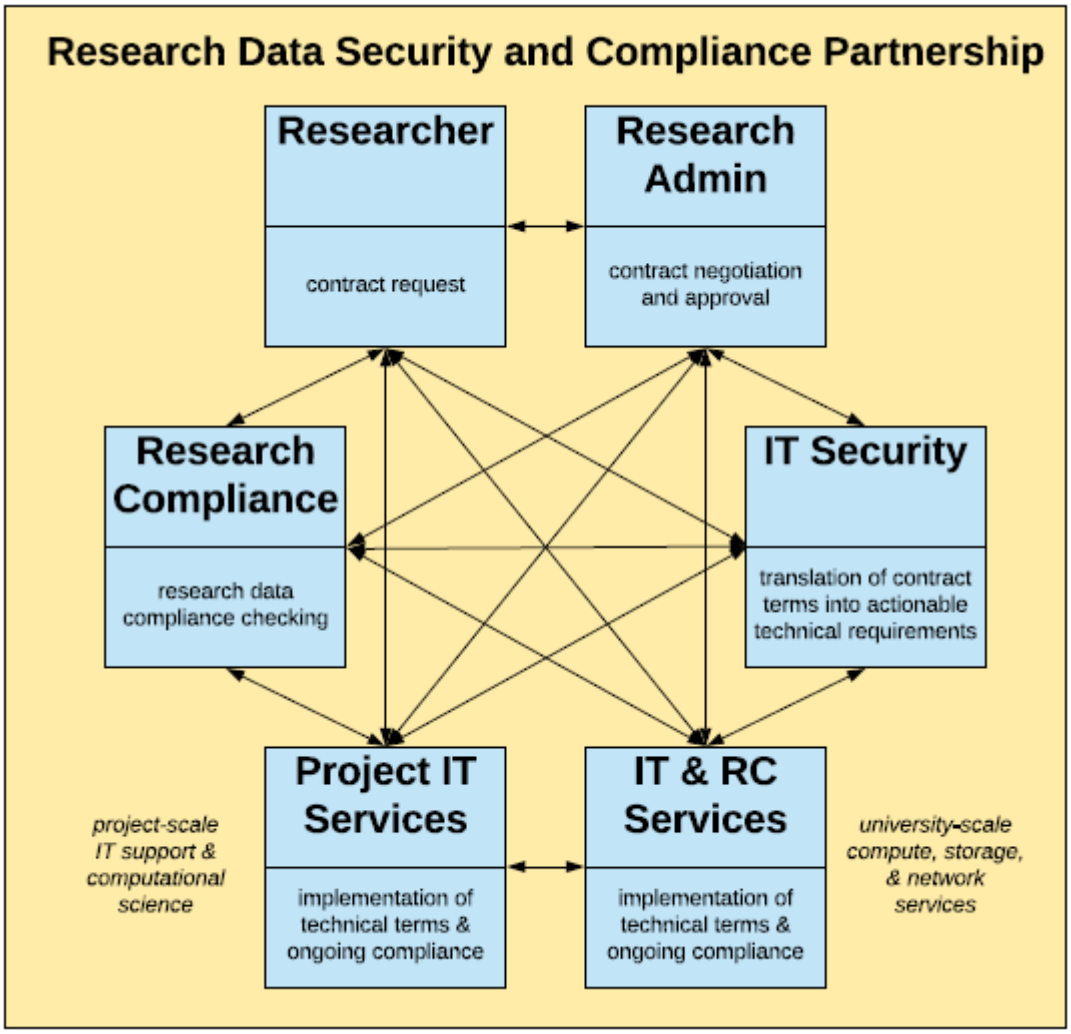
16:30 – 17:00 Validation, auditing, assessment, authorization

16:30 – 16:45	Colin Glover, colin.glover@sera-brynn.com Sera-Brynn, LLC	Flexible and Scalable Process for Assessing, Validating, Auditing, and Authorizing a HPC for Controlled Data
16:45 – 17:00	Joe Gridley, jdg284@psu.edu Penn State University	Validation of CUI Environments Using NIST 800-171A

ABSTRACTS

Greg Madden - Intra-Institutional Partnerships for Research Data Security and Compliance

At Penn State, research data security and compliance is a six-sided partnership that involves researchers, research administrators, IT security specialists, university-scale IT services, project-scale IT services, and research compliance specialists. Lack of coordination between any of the six parties can result in significant delays and/or wasted efforts at the start of research projects, either because projects are approved but the technical facilities for securing the data are not in place, or because the technical facilities are put in place but must sit unused while the project is approved. It is critical to solidify the internal relationships within the university and to ensure that every unit understands not only their own role, but the roles of their partners. Ultimately the goal is to create a systematic approach which results in a rapid flow from contract language to actionable technical requirements to implementation to approval, so that research data can be confidently acquired and research can begin in the minimum possible timeframe.



Preston Smith - Maturing REED from a Service to a Model

The Purdue REED system has been operational for over 2 years. In this presentation, we will share what we've learned through these efforts and how REED is evolving from a single cloud-based computing service to a one-stop ecosystem providing a campus model for addressing regulated research.

Ryan Gilmore - The role of the System Security Plan

The System Security Plan (SSP) documents the security posture of a system, defines roles and responsibilities for access to the system, and describes security controls currently implemented, are in the process of being implemented, and will be implemented in the future. It is a critical document which every system that processes, stores, or distributes data should have in its artifact repository. In addition, an SSP is required for systems to be compliant with NIST 800-171. This presentation will focus specifically on how to draft an SSP, provide insight on how to use an SSP to validate controls, and highlight lessons learned by the Institute for CyberScience at Penn State using this approach during a recent security controls validation event.

Mike Warfe - You want me to do what? Musings on writing a system security plan with labs.

The focus of this talk will be on outreach to faculty and labs regarding their responsibilities in writing system security plans. We will explore at the high level, responsibilities and approaches that one must take in order to ensure that the system security plan is scoped appropriately, communicated properly, and effective in execution.

Andrew Spragg – Strategic decisions in planning your SSP

Ensuring you create a strategy that aligns to the unique requirements of the data, sponsor, and auditors when planning and drafting an SSP. An approach to preparing for initial decisions of the requirements, sponsor expectations, delivery approach, and complexity in creating SSPs in unique data environments where utilizing strategic and critical decision making to create your organizational SSP strategy based on the requirements of unique situations.

Trey Breckenridge - Assured Compliance through Information Security Continuous Monitoring

Information Security Continuous Monitoring (ISCM) is defined by NIST as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. While monitoring for compliance is an objective in implementing an effective ISCM program, an effective ISCM strategy must also provide managers with a continuous means to assess overall security status in order to make informed and timely risk management decisions.

Maureen Dougherty - Building a Secure Data Environment

The University of Southern California's Center for High-Performance Computing provides a secure data environment for data analytics with their existing general purpose cluster resources. This service requires the deployment of open source tools, home grown code, and leveraging the Information Technology Service's Security department's expertise and their licensed applications. This presentation will review some of the technical aspects and challenges of our low-budget implementation.

Joe Gridley – Validation of CUI Environments Using NIST 800-171A

The recent release of NIST SP 800-171A has provided organizations some guidance on the government’s expectations for audit and validation practices. This session will briefly discuss the differences between 800-171A and 800-53A and explore lessons learned during the validation process, including when to validate, who should validate, and how to validate.