Validation of CUI Environments Using NIST 800-171A

Joseph Gridley, Esq., CIPP, CIPM, FIP
The Pennsylvania State University
Office of Information Security
jdg284@psu.edu

Objective

Answer the following questions:

- Why validate?
- What does it mean to validate?
- Who should validate
- When to validate?
- How to validate?

Why validate?

- NIST SP 800-171 3.12.1
  - “Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.”
- Hygiene?

What Does it Mean to Validate?

- Validation is:
  - Point in time evaluation of control status
- Validation is not:
  - Continuous monitoring
  - Security

Who Should Validate?

- Independent Validation and Verification
  - Internal Audit
  - 3rd Parties
  - Other?

When to Validate?

- NIST: “Periodically”
- FedRAMP: Annually
- After significant system changes

How to Validate?

- NIST 800-171A vs. NIST 800-53A
- Methods
  - Testing?
  - Interviews?
  - Document Review?
  - Spot Checks?

Resources

- BTAA NIST 800-171 Compliance Baseline
- FedRAMP
- NIST SP 800-171
- security@psu.edu