FEDERAL DEMONSTRATION PARTNERSHIP
Redefining the Government & University Research Partnership

Controlled Unclassified Information (CUI) and FISMA: an update

May 12, 2017

Mark Sweet, Nancy Lewis, Grace Park
Stephanie Gray, Alicia Turner

What is FISMA?

- Federal Information Security Modernization Act
- Defines how Federal information systems should be secured
- National Institutes of Standards and Technology (NIST) define the guidelines

FISMA vs. NIST

- FISMA gives the National Institutes of Standards and Technology (NIST) statutory responsibilities to establish non-product specific guidelines and standards to ensure a reasonable level of security in government systems

- The term “FISMA compliance” is often used to describe the process organizations go through to implement the NIST standards and guidelines

NIST Publications

- NIST publishes guidelines
- NIST SP 800-53: Federal systems
- NIST SP 800-171: Non-Federal systems

- These documents reference other NIST publications including Federal Information Processing Standards (FIPS)

NIST SP 800-171

- Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations

- Key document outlines measures to protect data and systems

CIA

- **C**onfidentiality
  - Data/system is protected
- **I**ntegrity
  - Data/system is not altered
- **A**vailability
  - Data/systems can be accessed for business

Security Requirement Families

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- System and Communications Protection
- System and Information Integrity

Example Controls

- **Access Control**
  - 3.1.13, Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- **Awareness and Training**
  - 3.2.3, Provide security awareness training on recognizing and reporting potential indicators of insider threat.
- **Audit and Accountability**
  - 3.3.2, Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
- **Incident Response**
  - 3.6.1, Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

Example Controls

- **Media Protection**:
  - 3.8.1, Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.
  - 3.8.3, Sanitize or destroy information system media containing CUI before disposal or release for reuse.
- **System and Information Integrity:**
  - 3.14.6, Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
  - 3.14.7, Identify unauthorized use of the information system.

Controlled Unclassified Information

- An open and uniform program to manage all unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy

Controlled Unclassified Information

- 32 CFR 2002 – Effective 11/14/2016
- Establishes policy for designating, handling, and decontrolling information that qualifies as CUI
- Goal to standardize how CUI is managed

Controlled Unclassified Information

- 32 CFR 2002 – Effective 11/14/2016

- Describes, defines, and provides guidance on the minimum protections for CUI
  - Physical and Electronic Environments
  - Destruction
  - Marking
  - Sharing

- Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)
  - These protections must continue as described in the underlying authorities.

Controlled Unclassified Information

- Two types of CUI
- CUI Specified: subset of CUI where there are governing laws requiring specific controls to manage (e.g. ITAR; HIPAA)
- CUI Basic: subset of CUI that is not Specified

Protecting CUI: summary

- Establish controlled environments
- Reasonably ensure unauthorized access does not occur
- Keep CUI under authorized control
- Protect confidentiality

Protecting CUI: summary

- Since we are (typically) not running a system for an agency CONFIDENTIALITY is the concern
- Integrity and Availability do not matter
  - Unless it matters to you!
- Confidentiality protections must be at the MODERATE level

Protecting CUI: summary

- Security requirements obtained from NIST SP 800 – 53
- Requirements tailored to streamline and remove controls that are (SP 800-171):

1. Uniquely Federal
2. Not protecting CUI Confidentiality
3. Routinely satisfied

Protecting CUI: summary

- CUI Basic: Confidentiality Moderate

- CUI Specified: may require Confidentiality, Integrity, Availability to be Moderate (or higher)

- Controls are the BASELINE

Current Activities

- Federal Government still working on implementing the full CUI program
- FAR 52.204-21 Basic Safeguarding of Covered Contractor Information
- Inconsistencies **within** and **among** Federal agencies
- FAR clause still under development
  - FDP institutions provided feedback to National Archives

University of Florida

UF Background: Major Milestones

- 2015
  - $40 million data analytics contract requires FISMA “moderate”
  - UF Research Shield goes “live” July 1, compliant with NIST 800-53 moderate
  - DFAR starts to require NIST 800-171
- 2016
  - UF Restricted Data Work Group formed to handle strategy and governance
  - UF Research Vault fit/gap for 800-171 requirements
  - Understanding 32 CFR 2002, what is CUI?
- 2017
  - Refine annual assessment process for UF Research Shied
  - Continue to address 800-171 gaps for UF Research Vault
  - $4.6 million contract requires FISMA “moderate” for animal study

UF IT Solutions – one size does not fit all

Solutions	Pros	Cons
Research Shield: compliant solution for research projects with complex collaborations and data processing	-Pre-assessed environment speeds up review/onboarding -Low cost to researcher due to institutional subsidy -Available now for projects with single user and software only	-Onboarding can take 1 – 4 months depending on complexity
Research Vault: compliant solution for research projects that only need to work with software/data storage/data processing	-Pre-assessed environment speeds up review/onboarding -Low cost due to researcher due to institutional subsidy -Available now for projects with single user and software only	-External devices or equipment cannot be used with ResVault -Complex collaborations or shared databases not supported until fall 2017
Pre-Built Computer Images: install pre-built configuration in a secure network environment	-Pre-assessed environment speeds up review/onboarding -Low cost, about the price of a new computer/laptop -Supports all special requirements, external devices -Linux and windows are supported -Local IT installs images and supports the machine	-Pre-Built images and secure network not available until summer 2017
Custom built computing environment	-Custom build supports all special requirements, external devices, etc -Local IT maintain and control the environment	-Requires full risk assessment, approx. 1 – 6 months -High cost since building from scratch

The challenge continues

- IT solutions – one size does not fit all, how do you build a compliant environment that scales to the majority of needs?
- Inconsistencies with contract terms and conditions – if you try to push back, but no luck, what then?
- Federal rules and IT standards are constantly evolving, how do you develop local strategy, process and policy that withstands the regulation "moving target"?

University of California - Irvine

UCI: The Long Road

- Late 2000s
  - NIH National Children's Study requires FISMA "moderate" (2007)
    - Secure environment provided by NIH
  - NIH Spinal Cord Injury Replication Animal Study requires FISMA "moderate" (2009)
    - Consulting company procured to build secure data center
- 2014
  - Data Use Agreements require various information security plans and/or certifications
- 2016-2017
  - Formation of UCI Research CyberInfrastructure (RCI)
    - Standing subcommittee reinstated
  - What is CUI?
    - What about student data?

UCI’s Approach to FISMA

- Contract and Grant Officers review Requests for Proposals, Contract Terms, and Data Use Agreement to identify FISMA requirements
- Information Security Officer(s) (“ISO”) are notified to assist with assessment of requirements and next steps
- C&G Officer works with the appropriate ISO and PI to negotiate the appropriate classification level
- ISO prepares the project specific addendum to the FISMA Core Security Plan for submission to Agency by C&G Officer
- ISO interacts with Agency ISO and Contracting Officer to finalize the plan as appropriate

UCI: Compliant Environments

- **Considerations**
  - Centralized vs. De-centralized
  - Cost
  - Buy-in
- **Options**
  - Cloud-based solutions
  - Local enclaves
  - Hybrid solutions

UCI: Challenges

- IT solutions – how do you design scalable options to fit researchers’ needs?
- Getting everyone (Sponsored Projects, IT, PIs) in the same room and on the same page

Institutional Perspectives

- Contract/Agreement Negotiations
- Institutional Buy In & Support
- Architecture & IT Implementation
- Policy Development
- Other Organizational Strategies/Risk Determination

Contact Information

- Mark Sweet, eRA Steering Committee Co-Chair; masweet@rsp.wisc.edu
- Stephanie Gray, University of Florida; slgray@ufl.edu
- Alicia Turner, University of Florida; aliciatu@ufl.edu
- Nancy Lewis, University of California – Irvine; nrlewis@uci.edu
- Grace Park, University of California – Irvine; parkgj@uci.edu