Controlled Unclassified Information (CUI)

APLU – CoR 2017 Summer Meeting

Panel Members

Greg Madden
Senior Advisor for Research Computing and Cyberinfrastructure
Office of the Vice President for Research
Penn State University
gem19@psu.edu

Lori Ann M. Schultz
Senior Director, Research Partnership Services
Research, Discovery & Innovation
University of Arizona
lschultz@email.arizona.edu

Alicia Turner
Business Relationship Manager
UFIT-Enterprise Systems
University of Florida
aliciatu@ufl.edu

Agenda

- Introduction
  - Controlled Unclassified Information (CUI)
  - Contracting
- CUI strategies for academic research
  - Pennsylvania State University
  - University of Arizona
  - University of Florida
- Q&A

Introduction:
CUI & Contracting

High Level CUI Timeline

- 2010 – Executive Order 13556 established Controlled Unclassified Information (CUI) Program
- 2015 – NIST published 800-171 for protecting CUI in non-federal systems
- 2015-16 - DFARS 252.204-7012 Interim Rules 1&2
- 2016 – 32 CFR Part 2002, final rule for CUI
- 2017 – pending CUI FAR clause

CONTROLLED UNCLASSIFIED INFORMATION

All **unclassified** inform
throughout th
that re g or

CUI does not apply DIRECTLY to non-federal entities, but INDIRECTLY applies by incorporating into contracts, grants, agreements, etc.

1. CUI Basic

Law/Reg/GW-P
informati
pr dy HOW

Examples: agriculture, water assessments, emergency management, visas, terrorist screening, death records

2. CUI Specified

Law/Reg/GW-Policy identifies an information type and says to protect it, and defines the security standards to protect the information

Examples: student records, nuclear, NATO restricted, DNA, export control, controlled technical information

Perhaps just as important, what is **not** CUI?

- CUI does NOT include:
  - Classified information
  - Information a non-executive branch entity possesses and maintains from its own systems that did not come from, or was not created for, or possessed by, an executive branch agency or entity acting for an agency
- "On behalf of" the Federal Government means:
  - Using or operating a Federal information system
  - Maintaining or collecting information for the purpose of processing, storing, or transmitting Federal information

CUI Registry – example 1

CUI Registry

Agriculture

Category-Subcategory:	**Agriculture**
Category Description:	Information related to the agricultural operation, farming or conservation practices, or the actual land of an agricultural producer or landowner.
Subcategory Description:	N/A
Marking:	AG

- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
7 USC 8791(b)	Basic	

CUI Registry – example 2

CUI Registry: Controlled Technical Information

Category-Subcategory: **Controlled Technical Information**

Category Description: Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

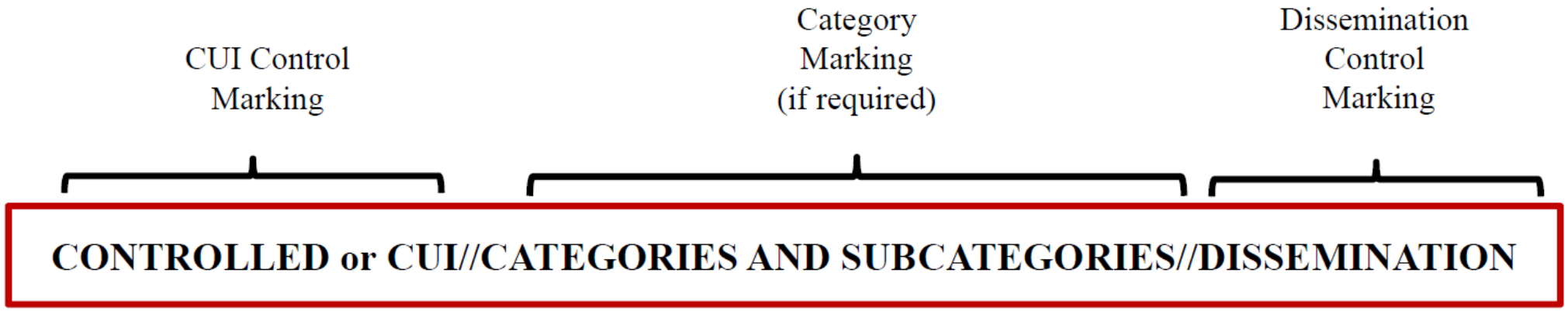
Subcategory Description: N/A

Marking: CTI

- **CUI Specified authorities include specific handling practices that differ from general CUI requirements. For Specified authorities, reference individual Safeguarding/Dissemination control citations for distinct requirements**
- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
48 CFR 252.204-7012	Specified	

CUI Marking – Banner Example



- See https://fas.org/sgp/cui/marking-2016.pdf
- Additional marking guidelines include:
  - Electronic media, forms, coversheets, presentations, transmittal documents, splash screens/db banners, room/areas, containers, shipping/mailing, legacy materials

Protecting Federal Information: Overview

- FISMA vs NIST
- Sample of NIST publications for protecting FEDERAL systems
  - FIPS199
  - FIPS200
  - 800-53
  - 800-37
  - 800-65

Other NIST Pubs

- NIST SP 800-37: Risk Management Framework
- NIST SP 800-65: Integrating IT Security into Capital Planning and Investment

Protecting CUI: NIST SP 800-171

- 800-171 overview
  - "Tailored" from FIPS200 and 800-53
  - Only focuses on protecting CONFIDENTIALITY at the MODERATE level
    - **But what about integrity??**
  - Non-tailorable requirements, but there is flexibility in how to meet the requirements

- Federal agencies must use 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems
  - Use 800-171 when non-fed receives CUI related to providing a service/product to the government **(i.e. conducting research)**
  - Do not use if collecting/maintaining CUI as part of gov function, builds/operates system for gov, or provides processing services **(800-53 applies instead)**

Contracting Basics

- 32 CFR 2002 only flows down when agencies include it
  - When new FAR becomes available, we expect to see it more (draft due in June)
- Agency-specific spin on 32 CFR 2002 (Dept of Homeland Security)
- DFARS 252.204-7012 comes from defense agencies and flow down to subcontractors

Contracting and DFARS 252.204-7012

- Read in conjunction with 252.204-7008 Compliance Clause
  - CDI and Fundamental research CANNOT coexist in a contract. **7012 is self-deleting** if work is fundamental research. Determination under 252.204-7000(a)(3) is critical.
  - Final rule **may** include carve out for fundamental research

- Primes should not flow down requirement unless subcontractor will be involved with CDI or operationally critical support

- When 7012 applies, DOD CIO must be notified of any NIST 800-171 requirements not implemented at time of award (30 days)

Be on the lookout

- New FAR clause for CUI
- DHS HSAR clause
- Final Rule for DFARS 252.204-7012

CUI Roles and Logistics:
Pennsylvania State University

CUI may involve many offices

- Whereas Open Data has compliance concerns but no security concerns…
- CUI has both compliance concerns AND security concerns
- Likely involves many campus offices acting together across the lifecycle of a research project

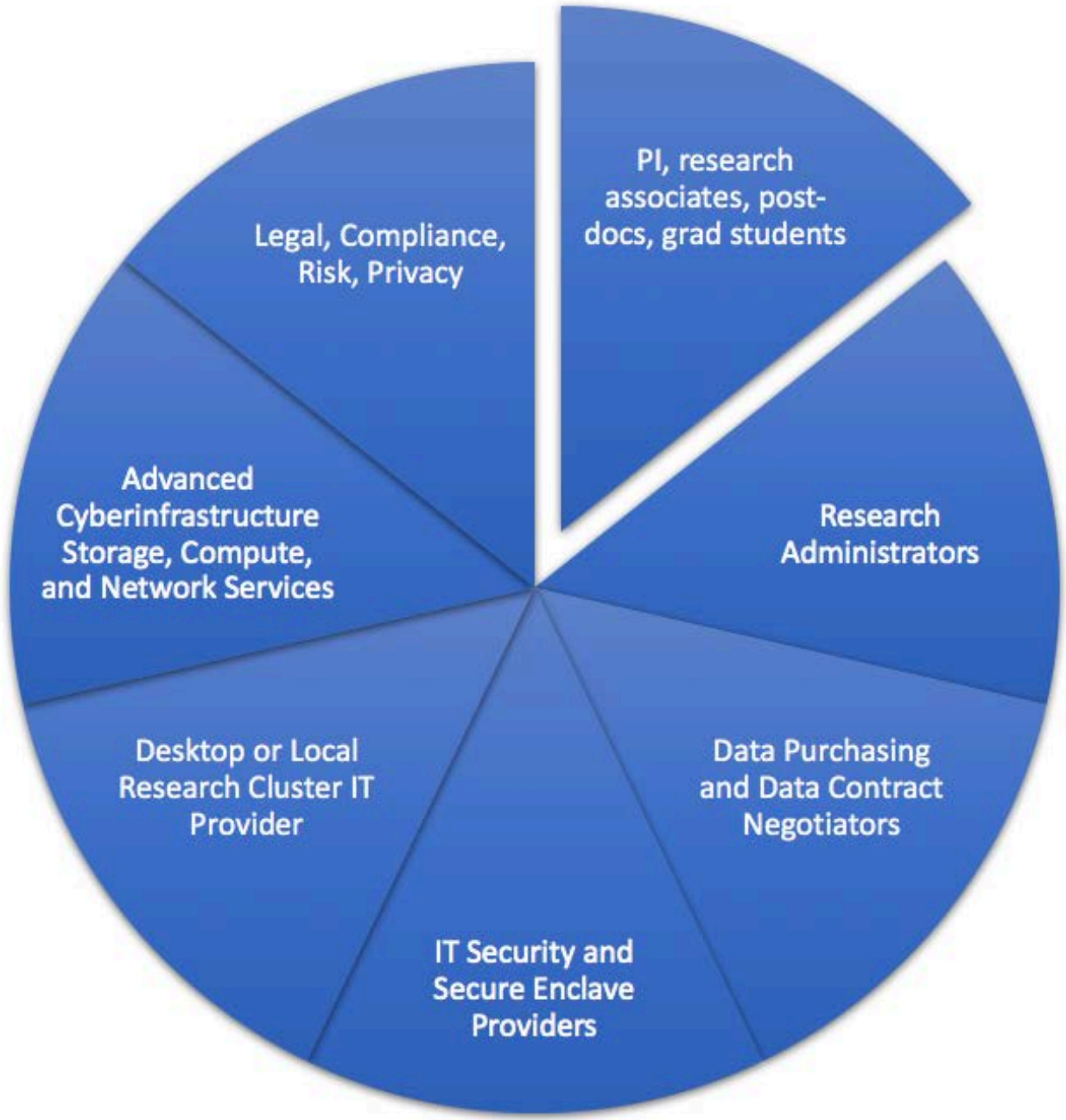
- Each stage of the research data technical lifecycle engages a different set of units…

Research Data Technical Lifecycle (1)

- Data Identification
  - PI, Research Methodology Centers, Grants and Contracts Offices, Sponsored Programs – anyone engaged in early project discussions
- Terms and Conditions
  - Negotiators, Sponsored Programs, Purchasing, Risk Management, General Counsel, PI, IT Security – as necessary
- Data Acquisition – Financial/Budgetary
  - PI, Grants and Contracts Offices, Purchasing – as necessary
- Data Acquisition – Technical
  - PI IT, Unit IT, Central IT, Research Network, Data Center, HPC Facility, Secure Enclave Service-- as necessary

Research Data Technical Lifecycle (2)

- Research Data Security and Compliance Planning
  - IT Security, Sponsored Programs, Research Protections, PI IT, Unit IT, Central IT, Data Center, HPC Facility, Secure Enclave Service
- Research Data Security and Compliance Implementation
  - Some subset of IT services
- Ongoing in-project security and compliance
  - Some subset of IT services, Research Protections
- Post-project Compliance – e.g. data destruction
  - Some subset of IT services, Sponsored Programs, Research Protections


PI, research associates, post-docs, grad students
Research Administrators
Data Purchasing and Data Contract Negotiators
IT Security and Secure Enclave Providers
Desktop or Local Research Cluster IT Provider
Advanced Cyberinfrastructure Storage, Compute, and Network Services
Legal, Compliance, Risk, Privacy

Importance of Early Recognition

- Due to potential technical complexity, helps to identify incoming CUI at the earliest stage
  - PI, Research Methodology Centers, Grants and Contracts Offices, Sponsored Programs – anyone engaged in early project discussions
- As secure enclaves are established, technical complexity of individual projects should decrease
- CUI projects have been time-challenged up to this point

Research Administrators

- Initiate the series of contacts that bring everyone into the loop…
- PI and research team– primary day-to-day responsibility for security and compliance
- IT Security – determines actionable technical requirements of contract terms
- Cyberinfrastructure Service Providers– implement technical requirements
  - PI IT, Unit IT, Central IT, VDI IT, HPC Facility, Server IT, Cloud IT, Data Center, Research Network
- Research Protections – ensures compliance over life of project
- Others as needed – Risk Management, General Counsel, Export Control, Privacy, etc.

IT Units

- Based on the research design and the IT structures in place, the data may end up on infrastructure controlled by PI IT, Unit IT, Central IT, Data Center Services, VDI IT, HPC facility, or Cloud provider
- At Penn State, not all IT service providers are equally adept at providing high-end security services
- May require education or supplemental technical staff to ensure security requirements are properly implemented
  - Particularly where IT is provided by grad students, post-docs, and research associates

Secure Repositories

- Permanent secure repositories can reduce the need for high-end IT security skills at the research project level
- Over time, the creation of secure repositories can reduce the technical complexity of individual projects by providing a reusable infrastructure
  - But they will need to be flexible enough to meet multiple research needs
- Identify existing secure repositories that meet the NIST guidelines
  - Convince them to share their infrastructure or knowledge with others
- Create centralized secure repositories
- Sponsored Programs and IT Security can be confident that the university will meet its security and compliance goals

Issues of Complexity

- Workflow tools across such a varied set of offices are not in place
- Processes are primarily person-based and email-based rather than institutionalized
- Even with every unit performing well, the sheer number of offices involved creates delays
- Communication is the key – even in the absence of processes or tools, simply gathering the various units together for frequent conversation increases the ability to meet the challenge

CUI strategies for academic research:
University of Arizona

UA Background: Major Milestones

- 2015
  - Received first subcontract with 7012 clause (we now have ~12)

- 2016
  - Formed working group to investigate/address NIST 800-171 requirements
  - Fit/gap analysis
  - August 2016: Budget approval for segmented environment for CUI projects
  - October 2016: AWS GovCloud pilot environment created

UA Background: Major Milestones

- 2017-18
  - April 2017: Browser client data transfer capability available
  - July 2017: Secure laptop loan capability available
  - November 2017: Assess compliance with NIST 800-171

- Throughout:
  - Communication/training
  - Implement compliant environment and onboard research
  - Assess compliance, training needs, costing and budgeting for future

UA environment: in progress

- Budget of $3.7M FY17-FY21
  - Personnel, equipment, cloud services, external professionals
  - Biggest challenge for many of us: monitoring/reporting incidents

- Still pending:
  - Assess scalability as new/more projects added
  - Costing for future proposals
  - Work with business affairs to assess need for recharge center

Addressing Burden

- Continuous review of requirements: CUI basic vs. CUI specified

- Communication and training to:
  - Faculty and local IT on use of environment
  - Contract analysts during negotiation, and resources available
  - Administrative staff on budgeting in future proposals

- Protection of ITAR and CDI:
  - Combine the TCP and 800-171 requirements review into one
  - Combine assessment with annual TCP review

CUI strategies for academic research:
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 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 of any size/complexity	-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 -Local IT installs images and supports the machine	-Pre-Built images and secure network not available until fall 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

UF solutions: cost rate

Solutions	Processor Core (RNCU)	Replicated Storage (RRSU)	User Fees
Research Shield	**$300 per RNCU** • One (1) priority dedicated CPU core configured with 4 GB of RAM • Approximately 3 GB per core usable by the software application	**$1,400 per RRSU** • One (1) TB of storage capacity (not use) with replication and tape backup • The second TB (for the replicated copy) is included	**$152 per User** • Covers software license fees
Research Vault	**$300 per RNCU** • One (1) priority dedicated CPU core configured with 4 GB of RAM • Approximately 3 GB per core usable by the software application	**$1,400 per RRSU** • One (1) TB of storage capacity (not use) with replication and tape backup • The second TB (for the replicated copy) is included	**$152 per User** • Covers software license fees

- For more information: https://www.rc.ufl.edu/services/rates/hardware-purchases/
- Additional notes
  - Cost for pre-configured desktop images is very low, about the price of a new desktop or laptop
  - Custom built solutions are very expensive, as you must build from scratch
  - Recent estimate from a FedRAMP certified vendor: $27,000/month

Lesson Learned: "Environmental Scan"

- Plan thoroughly before you build (4-6 months minimum)
- Form strategic planning group w/ major stakeholders early in the process
- Security controls 101
  - Take the time to learn them (all project stakeholders!)
  - Understand what you already have that can be leveraged
- Assess your research landscape
  - What volume requires information security scrutiny/interpretation?
  - What agencies can "talk NIST"?
- Design infrastructure/architecture that scales easily and builds in cost efficiencies

Lesson Learned: Governance

Policies and decisions

- Technical Owner
- Business owner
- Build or buy (cloud)
- Risk tolerance (i.e. who's in/out?)
- Cost model
- Institutional policies (i.e. mandated use)

Key stakeholders

- Faculty
- Vice President for Research
- Director of Sponsored Programs
- Chief Information Officer
- Chief Information Security Officer
- Research Computing Director
- Chief Privacy Officer
- General Counsel

Lesson Learned:
Process for Identifying & Onboarding

- How do you identify all research data that needs to be controlled?
  - Research Administrators and Contracts
  - Other “Triggers”
    - IRB
    - Export Review
    - ISM (Department Information Security Managers)
- How do you prioritize onboarding and track progress?
  - Governance team sets priorities
    - Size of award
    - Risk of data loss
    - Others?
  - Internal tracking systems

Lesson Learned:
Support the business, don't interrupt the business

- Train staff
  - Identify, interpret, negotiate "down or out"
  - Direct regulated data to the appropriate environment
- Best practices for efficient/expedient privacy and risk assessments
- Incorporate economic indicators to gauge financial loss/risk