Federal Cyber Requirements in Research Contracts

DFARS 252.204-7012 (Controlled Unclassified Information)

Dr. Hank Glaspie, Cyber Infrastructure Planning Manager

Ed Moses, Cyber Risk Assessor

Office of Cyber Risk Management (OCRM)

Office of Research & Graduate Studies (ORGS)

Oct 30, 2020

University of Central Florida

Agenda

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

- What is it
- Why do I need to know this
- How do I get compliant
- Consequences for Non-complinace
- The **FUTURE**

What is it

*** DoD Regulation to secure information/information systems to standards developed by the NIST – to provide:**

- **Adequate Security**
  - Protective measures against loss, misuse, unauthorized access to or modification of information
- **Covered Contractor Information System**
  - Unclassified Info System that Process, Store, or Transmit Covered Defense Information (CDI)
    - **Covered Defense Information (CDI)**
      - Controlled Technical Information (CTI) – military/space application
      - Other Information in **CUI** Registry (NARA)

What is CUI

- **Controlled Unclassified Information** (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. https://www.archives.gov/cui/about

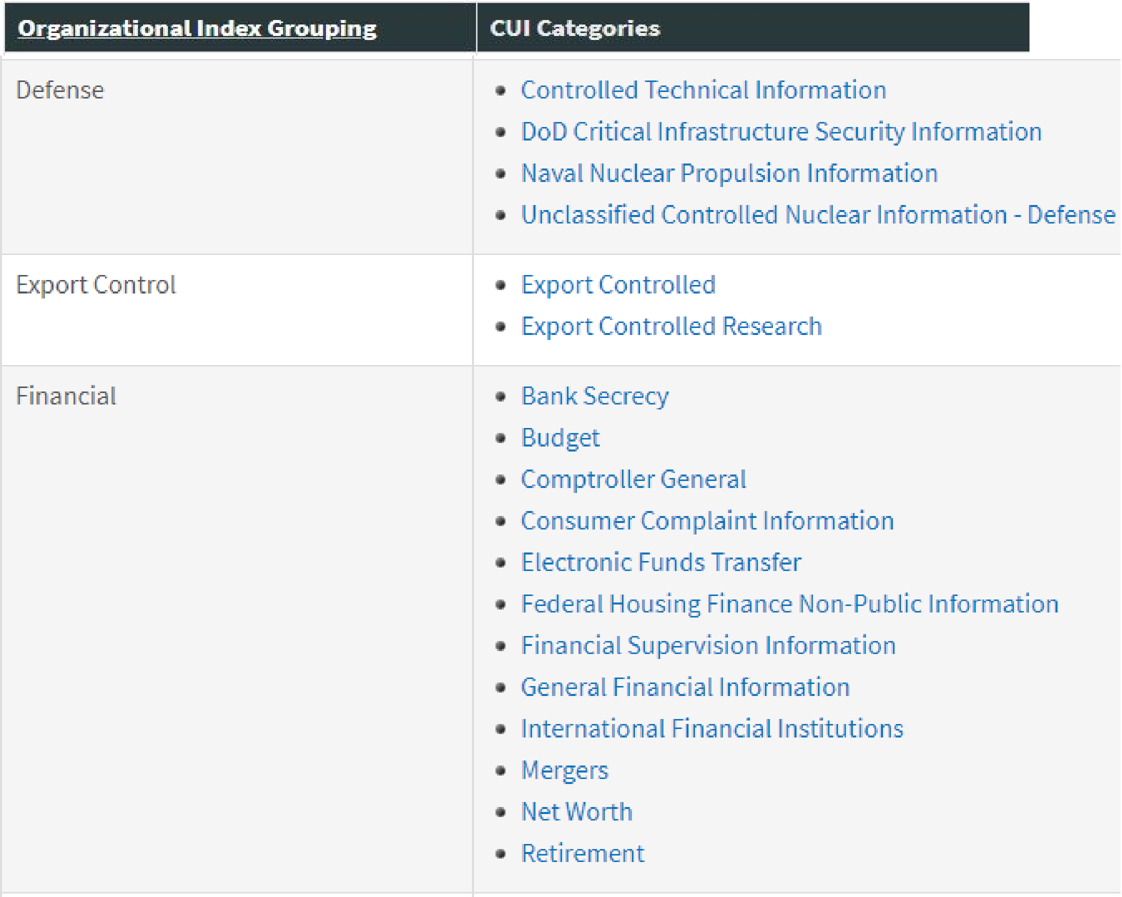
- CUI **replaces** For Official Use Only (**FOUO**) and Sensitive But Unclassified (**SBU**)…as well as LES, etc…
  - Clause NOT applied retroactively

- Covered under DODI 5200.48 dated March 6, 2020
  (replaces DoDM 5200.01 Vol 4)

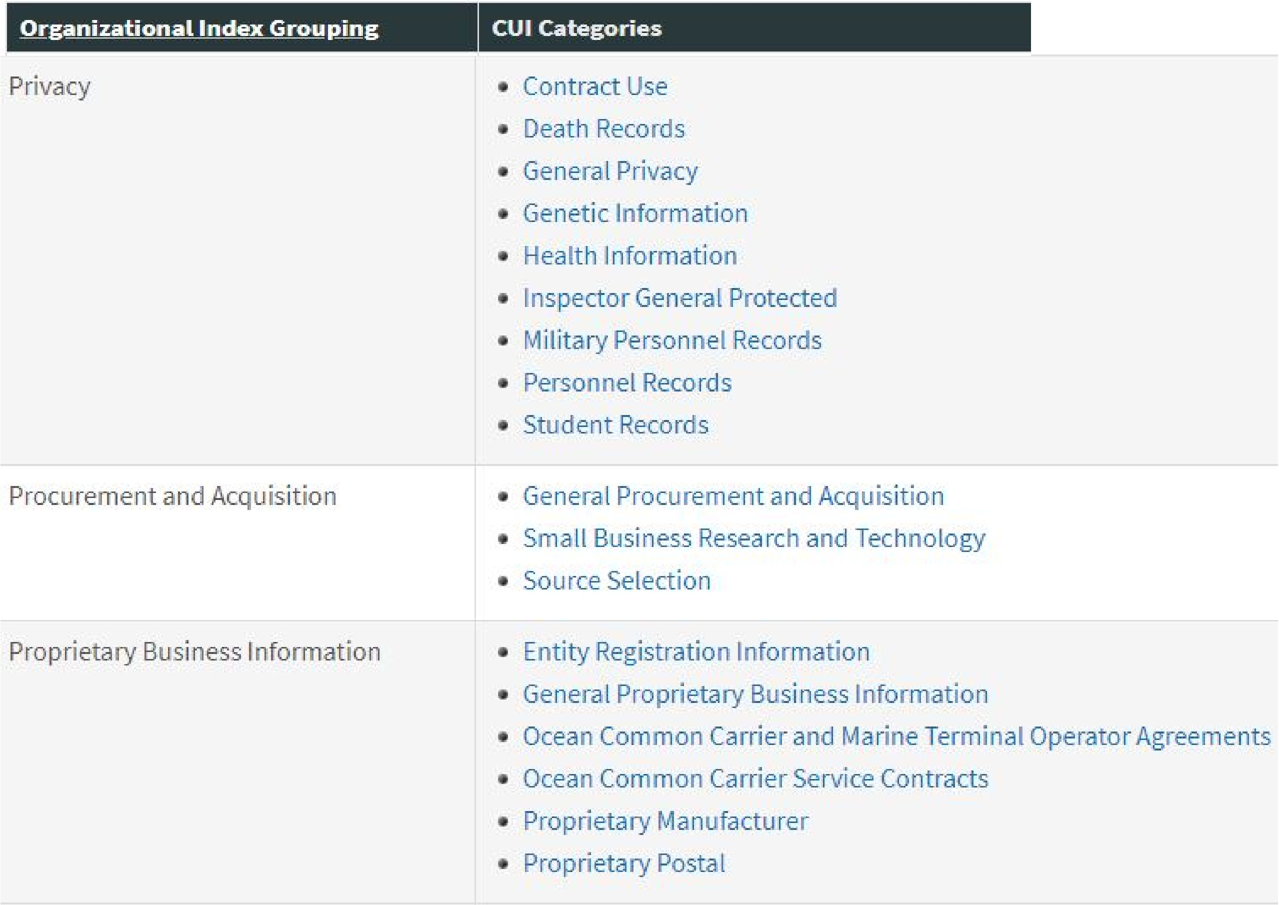
What is CUI

- Defined in the National Archives and Records Administration (NARA) CUI Registry
    - https://www.archives.gov/cui/registry/category-list
- Currently 20 Organizational Index Groupings
    - CUI Categories under each Grouping
        - EXAMPLE – Grouping /Category
            - PRIVACY / General Privacy
              / Health Information
              / Student Records

What is CUI



Organizational Index Grouping	CUI Categories
Defense	• Controlled Technical Information • DoD Critical Infrastructure Security Information • Naval Nuclear Propulsion Information • Unclassified Controlled Nuclear Information - Defense
Export Control	• Export Controlled • Export Controlled Research
Financial	• Bank Secrecy • Budget • Comptroller General • Consumer Complaint Information • Electronic Funds Transfer • Federal Housing Finance Non-Public Information • Financial Supervision Information • General Financial Information • International Financial Institutions • Mergers • Net Worth • Retirement



Organizational Index Grouping	CUI Categories
Privacy	• Contract Use • Death Records • General Privacy • Genetic Information • Health Information • Inspector General Protected • Military Personnel Records • Personnel Records • Student Records
Procurement and Acquisition	• General Procurement and Acquisition • Small Business Research and Technology • Source Selection
Proprietary Business Information	• Entity Registration Information • General Proprietary Business Information • Ocean Common Carrier and Marine Terminal Operator Agreements • Ocean Common Carrier Service Contracts • Proprietary Manufacturer • Proprietary Postal

Partial List of CUI Registry
* (From NARA)

Why do I need to know this

- Required Since Dec 31, 2017
- Better understanding of risks posed by threats and vulnerabilities
- Need to abide by federal regulations and guidelines
- **It is in some of the contracts that are signed**

How do I get -- COMPLIANT

- **Clause** needs to be in RFP/Contract **AND** CUI needs to be collected, **DEVELOPED**, received, transmitted, used, or stored by or on behalf of DoD

- **Exception** – Fundamental Research **

- **Adequate Security**
  - NIST SP 800-171 (Non-Federal System)
  - FedRAMP Moderate or equivalent (External Cloud)
  - Breach reporting within 72 hours of discovery
  - Forensic preservation if a breach occurs

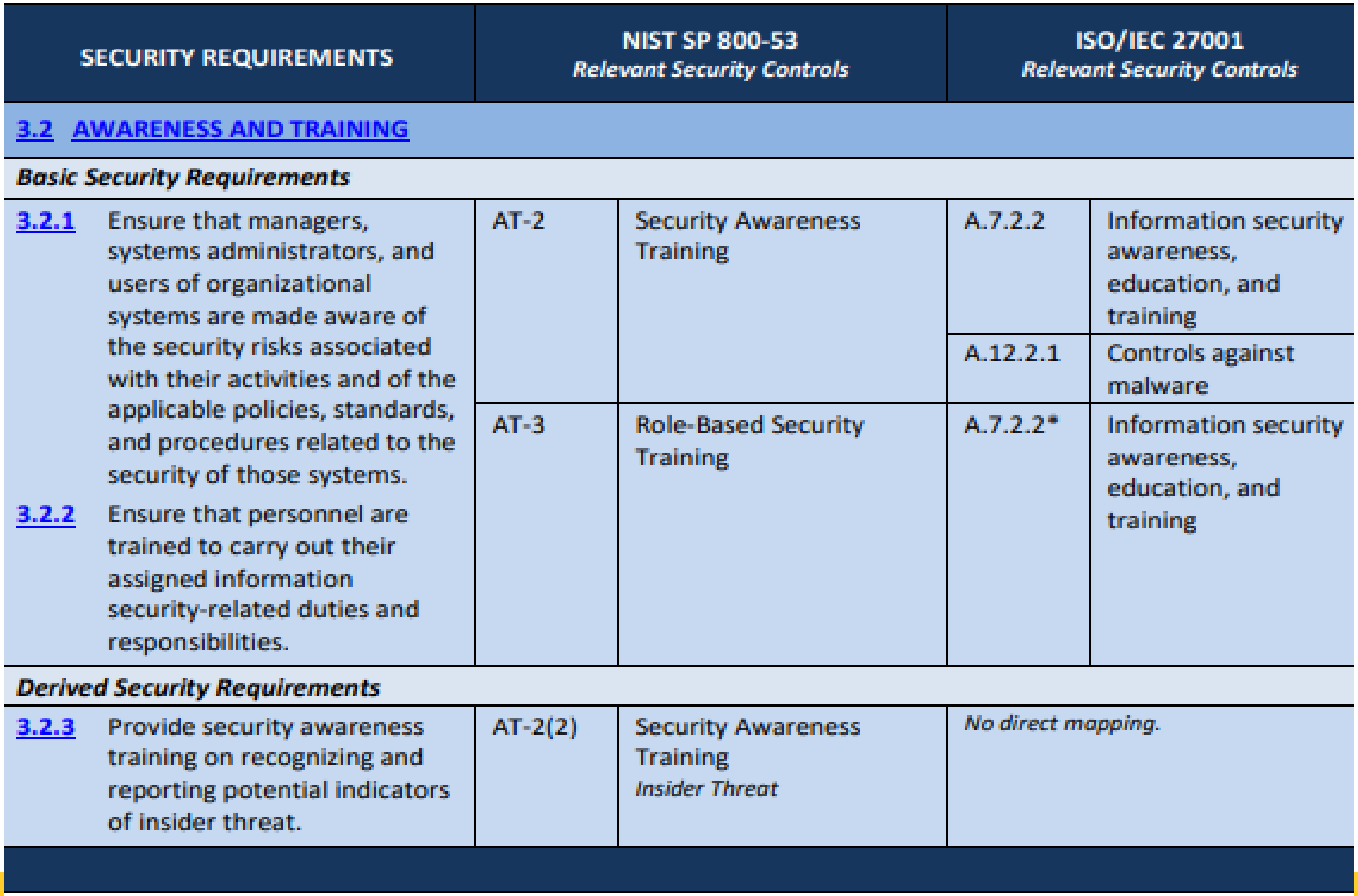
How do I get -- COMPLIANT

- **LAN / Self Contained**
  - **NIST SP 800-171**
    - **Develop an SSP & POA&M**
    - **SSP (System Security Plan)**
      - 110 Controls (NIST SP 800-171)
      - Hardware & Software list
      - Network Diagram

How do I get -- COMPLIANT

- **Example of the Controls (From NIST SP 800-171)**

TABLE D-2: MAPPING AWARENESS AND TRAINING REQUIREMENTS TO CONTROLS



SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.2	AWARENESS AND TRAINING				
Basic Security Requirements					
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	AT-2	Security Awareness Training	A.7.2.2	Information security awareness, education, and training
				A.12.2.1	Controls against malware
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	AT-3	Role-Based Security Training	A.7.2.2*	Information security awareness, education, and training
Derived Security Requirements					
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training *Insider Threat*	*No direct mapping.*	

How do I get -- COMPLIANT

- **POA&M (Plan of Action & Milestones)**
  - Identify controls not implemented and plan on when & how they will be implemented

- We (OCRM) have templates for these 2 documents (collaborative effort)

- **CLOUD**
  - **Controlled AWS FedRAMP Environment - CAFÉ**
    - GRIT and OCRM will assist

- Self – Attestation (not happening) - The Future

Consequences for Non-Compliance

- Government issue a stop work order until compliant
- Fines (Breach of Contract, False Claims Act, etc..)
- Loss of Future Work
- PI & University Reputation
- Loss of Data and Intellectual Property

The FUTURE

- **CMMC (Cybersecurity Maturity Model Certification)**

- DoD – in all RFPs by 2025
  - Need to be 100% compliant
  - NO POA&M

- Levels 1-5 (low to high security)
  - Level 3 = CUI
    - 110 controls + additional 20 = 130 total

- Will require external 3rd Party Certification/Accreditation
  - Approved Vendor List

The FUTURE

- **Senate Legislation**
  - Consumer Data Privacy and Security Act of 2020 (March 2020)

- Dept of Education
  - Strongly encouraged institutions to follow NIST SP 800-171 in handling student information

***** THE FUTURE IS NOW --- DFARS INTERIM RULE**

DFARS Interim Rule - 252.204-7019, 7020, & 7021

- **Purpose:** Assess contractor implementation of Cybersecurity requirements
- **Dates:** Released September 29, 2020 and Effective *November 30, 2020*
- **Affects:** New awards and modifications to existing DoD awards
- **Introduces:**
  - Assessment Methodology
    - Three levels: Basic, Medium, High
  - Cybersecurity Maturity Model Certification (CMMC) framework
    - Notice of DoD roll out of CMMC; when DoD identifies contracts that require immediate CMMC certification, it must be attained for award. Contractors encouraged to move towards compliance
- **Requires:**
  - Basic assessment score reported in Supplier Performance Risk System (SPRS) by Nov 30 and updated every 3 years (at a minimum) – by CAGE code and System Security Plan
  - Primes to ensure whole supply chain have submitted Basic score in SPRS by award

DFARS: Assessment Methodology

- **Basic** (performed by contractor, per SSP/environment)
  - Each of the 110 controls in NIST 800-171 is assigned a point value (5, 3, or 1)
  - Based on self-assessment, point value for each unimplemented control is subtracted from 110
    - *Possible to get a score of 0, even a negative score!*
  - Score must be reported in SPRS, provides LOW level of confidence to government
- **Medium** (performed by Defense Industrial Base Cybersecurity Assessment Center (DIBCAC))
  - Government conducts review of System Security Plan
    - May do phone interview and spot checks
  - Provides MEDIUM level of confidence to government
- **High** (performed by Defense Industrial Base Cybersecurity Assessment Center (DIBCAC))
  - Government conducts assessment either on-site or virtual to verify, examine, and review demonstration of the contractor's System Security Plan
  - Provides HIGH level of confidence to government

DFARS Interim Rule Implications

- Perform a self-assessment using NIST 800-171 Scoring Methodology
  - (Score attained from your SSP)

- https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html

- Report basic score into the Supplier Performance Risk System (SPRS) by November 30th

- Responsible to confirm your supply chain is also adhering to requirement

Conclusion

- Not here to prevent work but continue work and stay compliant with Federal Regulation
- Security = Mitigating Risk
- **You Are NOT alone**
  - **UCF NIST Working Group**

Risk can never be eliminated and so it must be MANAGED!!

Questions

Contact Us:

ResearchOCRM@UCF.EDU