Controlled Unclassified Information: Higher Education Perspective

David Brady
Impact of Export Controls on Higher Education and Scientific Institutions
May 24, 25, 2016
Scope: When are these controls required?

- Higher Ed concludes:

- Agreement directly references NIST 800-171.

- Data Sharing Agreement or Confidential Disclosure Agreement references security requirements in NIST 800-171.
Scope: When are these controls required?

- Higher Ed concludes:

- DoD Contract after August 26, 2015 has DFARS 252.204-7012 Safeguarding clause (August, September, October, December 2015 versions) and Covered Defense Information.

- DoD Solicitations after August 26, 2015 has DFARS 252.204-7008 Safeguarding clause (August, September, October, December 2015 versions). **MAYBE.**
Scope: When are these controls required?

- Higher Ed concludes **NOT WHEN:**

  - Federal contract or flowdown after May 16, 2016 has FAR clause **52.204–21 Basic Safeguarding of Covered Contractor Information Systems.**
  - Clause implements 15 controls on “covered contractor information systems” with “federal contract information”
  - Control xi may be problematic
  - **CUI FAR Clause will override this clause**
52.204–21 Basic Safeguarding of Covered Contractor Information Systems.

- Controls:
  
  - (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

  - (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

  - (iii) Verify and control/limit connections to and use of external information systems. (iv) Control information posted or processed on publicly accessible information systems.

  - (v) Identify information system users, processes acting on behalf of users, or devices.
52.204–21 Basic Safeguarding of Covered Contractor Information Systems.

- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

- (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
52.204–21 Basic Safeguarding of Covered Contractor Information Systems.

- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

- (xii) Identify, report, and correct information and information system flaws in a timely manner.

- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

- (xiv) Update malicious code protection mechanisms when new releases are available.

- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.
Why is this a Big Deal for Higher Ed?

- **Before:** We were told to protect information, and for the most part, you chose how.

**Now:** There are a defined set of required information security controls to protect controlled unclassified information.

- Requirements **will likely** require additional personnel or other resources to meet.

- If the requirements cannot be met, the university cannot and will not enter into the binding agreement (e.g. data sharing agreement, research contract, etc.) resulting in the loss of research funds or information necessary for university operations.
What are the requirements of NIST 800-171?

- 109 Individual Controls

- Technology-driven controls (e.g., audit logging, two factor authentication, password controlled screensavers)

- 80+ policy-based controls (e.g., controlling connection to mobile devices)

- Training controls (Information related security training, security awareness training- insider threat)

- All controls are requirements, unless exceptions are granted by federal agency providing oversight.
What are the requirements of NIST 800-171?

- DFAR 252.204-7012 (DEC 2015) specific requirements

- Controls not met:
  Reporting to DoDCIO: 30 days after contract-number of controls not met on contract award that will be met by December 2017

- Cyber Incident Report:
  Reporting to DIBNet: 72 hours after intrusion detected on information system with CDI (20 items, what happened and how it happened)
DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident.

1. Company name
2. Company point of contact information (address, position, telephone, email)
3. Data Universal Numbering System (DUNS) Number
4. Contract number(s) or other type of agreement affected or potentially affected
5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
6. USG Program Manager point of contact (address, position, telephone, email)
7. Contact or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
8. Facility CAGE code
9. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
10. Impact to Covered Defense Information

Source: DiBNet
DFAR 252.204-7012 (DEC 2015) specific requirements:
Cyber Incident Report

- DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident.

Impact to Covered Defense Information
11. Ability to provide operationally critical support
12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)
19. Incident/Compromise narrative
20. Any additional information

Source: DiBNet
What are the requirements of NIST 800-171?

High Impact Controls

1. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
2. Monitor and control remote access sessions.
3. Route remote access via managed access control points.
4. Authorize wireless access prior to allowing such connections.
5. Control connection of mobile devices.
7. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

Source: TJ Beckett
What are the requirements of NIST 800-171?

High Impact Controls

8. Review and update audited events.


10. Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.

11. Provide audit reduction and report generation to support on-demand analysis and reporting.

12. Protect audit information and audit tools from unauthorized access, modification, and deletion.

13. Limit management of audit functionality to a subset of privileged users.

Source: TJ Beckett
What are the requirements of NIST 800-171?

**High Impact Controls**

14. Track, review, approve/disapprove, and audit changes to information systems.

15. Analyze the security impact of changes prior to implementation.

16. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

17. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

18. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

19. Control the use of removable media on information system components.

20. Prohibit the use of portable storage devices when such devices have no identifiable owner.

Source: TJ Beckett
What are the requirements of NIST 800-171?

High Impact Controls

21. Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

22. Control information posted or processed on publicly accessible information systems.

23. Maintain audit logs of physical access.

24. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

25. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

26. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Source: TJ Beckett
CUI- Export Compliance Implications

- **CUI Basic**: A category or subcategory of CUI listed on the NARA CUI Registry for which NIST 800-171 security requirements apply.

- **CUI Specified**: A category or subcategory of CUI listed on the NARA CUI Registry for NIST 800-171 security requirements do not apply because there are already security requirements “specified” other than NIST 800-171.

- The CUI Specified categories and subcategories are marked on the registry with an asterisk (*).

- *Use the category/subcategory citations to determine if your CUI is Basic or Specified*
CUI- Description vs. Regulation

- CUI category and subcategory descriptions are not “legal definitions”

- However, at least one agency (DoD) has used a CUI Registry definition (export controls) in a recent regulation - despite the public’s objections

Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.

- The new regulation definition exceeds statutory authority

- What is NARA going to do to fix this?
Recommendations for FAR Clause Implementation

- Start with a Notice of Proposed Rulemaking (NOPR)-how much CUI is out there?

  Until you know that, you cannot evaluate the significance of impacts of the rulemaking

- Propose phased implementation- to contractors this is a potential change of the magnitude that FISMA was to the USG

  Compliance implementation could take years.
Recommendations for FAR Clause Implementation

- Not all CUI is the same

  Be prepared to answer why EAR99 CUI has to be protected at the level of protection (NIST 800-171) that ITAR CUI does

- Establish a baseline for existing controls—for each category and subcategory citation—what are the controls in place?

  Until you know what the gap is between the existing controls and NIST 800-171, you cannot evaluate the significance of impacts of the rulemaking
Confusing Terminology

- CUI and Safeguarding terms: “Basic” are not consistent

- “CUI Basic” (NARA CUI Registry)
- “Basic Safeguarding” (FAR 52.204-21) is not the same as “Basic Safeguarding (NIST 800-53)

“Basic Safeguarding” does not apply to “CUI Basic”- very confusing to higher ed
Questions?
What type of information is categorized as CUI?

Agriculture

- Information related to the agricultural operation, farming or conservation practices, or the actual land of an agricultural producer or landowner.
What type of information is categorized as CUI?

Controlled Technical Information*

- 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.
What type of information is categorized as CUI?

Critical Infrastructure

- Subcategories:
  - Ammonium Nitrate
  - Chemical terrorism-Vulnerability Information*
  - Critical Energy Infrastructure Information
  - DoD Critical Infrastructure Security Information
  - Physical Security*
  - Protected Critical Infrastructure Information*
  - Water Assessments

- Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.
What type of information is categorized as CUI?

Emergency Management

- Related to information concerning the continuity of executive branch operations during all hazards emergencies or other situations that may disrupt normal operations.
What type of information is categorized as CUI?

Export Control*

- Subcategories:
  - Research

- Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the ammunitions list; license applications; and sensitive nuclear technology information.
What type of information is categorized as CUI?

Financial*

- Subcategories:
  - Bank Secrecy
  - Budget
  - Central Contractor Registration
  - Commodity
  - Comptroller General
  - Electronic Funds Transfer
  - International Financial Institutions
  - Mergers
  - Retirement

- Related to the duties, transactions, or otherwise falling under the purview of financial institutions or United States Government fiscal functions. Uses may include, but are not limited to, customer information held by a financial institution.
What type of information is categorized as CUI?

Foreign Government Information*

- Information provided by, otherwise made available by, or produced in cooperation with, a foreign government or international organization.
What type of information is categorized as CUI?

Geodetic Product Information

- Related to imagery, imagery intelligence, or geospatial information.
What type of information is categorized as CUI?

Immigration

- Controlled at the Subcategory level only.

- Subcategories:
  - Asylee
  - Battered Spouse or Child
  - Permanent Resident Status
  - Status Adjustment
  - Temporary Protected Status
  - Victims of Human Trafficking
  - Visas

- Related to admission of non-US citizens into the United States and applications for temporary and permanent residency.
What type of information is categorized as CUI?

Information Systems Vulnerability Information

- Related to information that if not protected, could result in adverse effects to information systems. Information system means a discreet set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
What type of information is categorized as CUI?

Intelligence

- Subcategories:
  - Financial Records*
  - Foreign Intelligence Surveillance Act
  - Foreign Intelligence Surveillance Act Business Records
  - National Security Letter
  - Terrorist Screening

- Related to intelligence activities, sources, or methods.
What type of information is categorized as CUI?

**Law Enforcement**

- **Subcategories:**
  - Campaign Funds
  - Committed Person
  - Communications
  - Criminal History Records Information*
  - DNA*
  - Financial Records*
  - Informant
  - Investigation
  - Juvenile
  - National Security Letter
  - Pen Register/Trap & Trace
  - Reward
  - Sex Crime Victim
  - Terrorist Screening
  - Whistleblower Identity

Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions.
What type of information is categorized as CUI?

Legal

- Controlled at the Subcategory level only.

- Subcategories:
  - Administrative Proceedings*
  - Child Pornography*
  - Child Victim/Witness
  - Collective Bargaining
  - Federal Grand Jury*
  - Presentence Report
  - Prior Arrest
  - Privilege
  - Protective Order*
  - Victim
  - Witness Protection*

- Information related to proceedings in judicial or quasi-judicial settings. applications for temporary and permanent residency.
What type of information is categorized as CUI?

North Atlantic Treaty Organization (NATO)

- Controlled at the Subcategory level only.

- Subcategories:
  - NATO Restricted
  - NATO Unclassified

- Related to information generated by North Atlantic Treaty Organization (NATO) member countries under the North Atlantic Treaty international agreement, signed on April 4, 1949.
What type of information is categorized as CUI?

Nuclear*

- Subcategories:
  - Naval Nuclear Propulsion Information
  - Safeguards Information*
  - Security Related Information*
  - Unclassified Controlled Nuclear Information Defense*
  - Unclassified Controlled Nuclear Information Energy*

- Related to protection of information concerning nuclear reactors, materials, or security.
What type of information is categorized as CUI?

Patent

- Controlled at the Subcategory level only.

- Subcategories:
  - Application*
  - Invention
  - Secrecy Orders

- Patent is a property right granted by the Government of the United States of America to an inventor "to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States" for a limited time in exchange for public disclosure of the invention when the patent is granted.
What type of information is categorized as CUI?

Privacy

- Subcategories:
  - Contract Use
  - Death Records
  - Genetic Information*
  - Health Information*
  - Inspector General*
  - Military
  - Personnel*
  - Student Records*

- Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M0716, or "means of identification" as defined in 18 USC 1028(d)(7).
What type of information is categorized as CUI?

Procurement and Acquisition*

- Subcategories:
  - Small Business Research and Technology
  - Source Selection*

- Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.
What type of information is categorized as CUI?

Proprietary Business Information*

- Subcategories:
  - Manufacturer
  - Postal
  - Service Contract
  - Small Business Research and Technology
  - Source Selection

- Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.
What type of information is categorized as CUI?

SAFETY Act Information

- Defined as “SAFETY Act Confidential Information” in 6 CFR Part 25, the regulations implementing the Support Antiterrorism by Fostering Effective Technologies Act of 2002, SAFETY Act Information includes any and all information and data voluntarily submitted to the Department of Homeland Security under this part (including Applications, Pre-Applications, other forms, supporting documents and other materials relating to any of the foregoing, and responses to requests for additional information), including, but not limited to, inventions, devices, Technology, knowhow, designs, copyrighted information, trade secrets, confidential business information, analyses, test and evaluation results, manuals, videotapes, contracts, letters, facsimile transmissions, electronic mail and other correspondence, financial information and projections, actuarial calculations, liability estimates, insurance quotations, and business and marketing plans.
What type of information is categorized as CUI?

Statistical*

- Subcategories:
  - Census
  - Investment Survey
  - Pesticide Producer Survey

- Refers to information collected by a Federal statistical agency, unit, or program for statistical purposes or used for statistical activities; under law, regulation, or Government-wide policy such 'Statistical' CUI requires: (1) protection from unauthorized disclosure; (2) special handling safeguards; and/or (3) prescribed limits on access or dissemination.
What type of information is categorized as CUI?

Tax*

- Subcategories:
  - Convention

- Related to a compulsory contribution to government revenue involving information regarding returns or taxpayers.
What type of information is categorized as CUI?

Transportation

- Controlled at the Subcategory level only.

- Subcategories:
  - Sensitive Security Information*

- Related to any mode of travel or conveyance by air, land, or waterway.