The Impact of Federal Protected Information Regulations on Higher Education Institutions

American Society for Engineering Education
March 13, 2018

Doug Backman
University of Central Florida
The Impact of Federal Protected Information Regulations on Higher Education Institutions

WELCOME

Doug Backman, Director
Office of Compliance
Office of Research & Commercialization
(407) 882-1168
dbackman@ucf.edu
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Agenda

- Controlled Unclassified Information (CUI)

- National Institute of Standards & Technology (NIST) Special Publication 800-171

- Safeguarding Covered Defense Information and Cyber Incident Reporting - 252.204-7012
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Controlled Unclassified Information (CUI)

- National Archives & Records Administration (NARA)
- CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or Government – wide policy requires an agency to handle using safeguarding or dissemination controls
- The NARA CUI program establishes policies and standardizes the way the executive branch handles information that requires protection under laws, regulations or Government-wide policies.
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Controlled Unclassified Information (CUI)

- Prior to the CUI Program agencies employed *ad hoc*, agency specific policies, procedures and markings to handle CUI information.
- The NARA final rule consolidates all control requirements under one guideline that applies to all Executive Agencies
- CUI Registry
The Impact of Federal Protected Information Regulations on Higher Education Institutions

CUI Registry - Categories and Subcategories

***** IMPLEMENTATION REMINDER FROM THE EXECUTIVE AGENT *****
Existing agency policy for all sensitive unclassified information remains in effect until your agency implements the CUI program. Direct any questions to your agency's CUI program office.

Search the Registry [GO]

CUI Categories and Subcategories

- Select a Category or Subcategory to view associated detail information.
- Unless noted, CUI may be controlled at the Category or the Subcategory level.

<table>
<thead>
<tr>
<th>Category</th>
<th>Category Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture</td>
<td>Information related to the agricultural operation, farming or conservation practices, or the actual land of an agricultural producer or landowner.</td>
</tr>
<tr>
<td>Controlled Technical Information</td>
<td>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</td>
</tr>
</tbody>
</table>
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Controlled Unclassified (CUI) Registry

[https://www.archives.gov/cui/registry/category-list](https://www.archives.gov/cui/registry/category-list)

Agriculture
Controlled Technical Information
Critical Infrastructure
Emergency Management
Export Control
Financial
Geodetic Product Information
Immigration
Information Systems Vulnerability Information
Intelligence
Proprietary Business Information
Tax

International Agreements
Law Enforcement
Legal
National & Cultural Resources
NATO
Nuclear
Patent
Privacy
Procurement & Acquisition
SAFETY Act Information
Statistical
Transportation
CUI Registry: Export Control

<table>
<thead>
<tr>
<th>Category-Subcategory:</th>
<th>Export Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Description:</td>
<td>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.</td>
</tr>
<tr>
<td>Subcategory Description:</td>
<td>N/A</td>
</tr>
<tr>
<td>Marking:</td>
<td>EXPT</td>
</tr>
</tbody>
</table>

- 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.

<table>
<thead>
<tr>
<th>Safeguarding and/or Dissemination Authority</th>
<th>Basic or Specified</th>
<th>Sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 USC 4614(c)</td>
<td>Basic</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>13 USC 3801(g)</td>
<td>Basic</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>15 CFR 726. Subpart No. 770</td>
<td>Specified</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>22 CFR 124.9(e)(5)</td>
<td>Basic</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>22 CFR 126.10(b)</td>
<td>Specified</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>50 USC 4605(j)(5)</td>
<td>Basic</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>15 CFR 748.1(c)</td>
<td>Specified</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>15 CFR 760.5(c)</td>
<td>Specified</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>10 USC 130(a)</td>
<td>Basic</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>32 CFR 250.4(a)</td>
<td>Basic</td>
<td>22 CFR 127.3</td>
</tr>
<tr>
<td>32 CFR 250.9</td>
<td>Specified</td>
<td>22 CFR 127.3</td>
</tr>
</tbody>
</table>

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Controls/Safeguarding

- Controls – safeguarding or dissemination controls that a law, regulation or Government-wide policy requires agencies to follow.

- CUI Safeguarding Standards – Authorized holders (of the information) must safeguard CUI using one of the following types of standards (Control Levels)
  - CUI Basic – no special handling requirements for agencies.
  - CUI Specified – requires agencies to control or protect information and provide specific controls for doing so. Includes authorizing law, regulation or Government-wide policy containing specific handling controls.
  - CUI non-Specified – agencies provide some of the controls and specify only some of the controls.
The Impact of Federal Protected Information Regulations on Higher Education Institutions

CUI - Safeguarding and Dissemination

- Safeguarding
  - NIST policy standards
  - Authorized Holders
  - Control Environments
  - Protect Confidentiality
  - Reproducing CUI Standards
  - Destroying CUI
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Information System Control Requirements

- Non-Federal Information Systems
  - CUI Basic requires the controls outlined under NIST SP 800-171 – (110 Controls)
  - CUI Specified requires NIST SP 800-171 plus any special requirements – (110 – 125 Controls)

- Federal Information Systems
  - NIST SP 800-53 – (125 Controls)
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Information System Requirements

- Federal Information Systems – used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

- Non-Federal Information System – any system that does not meet the criteria for a Federal information system. When a non-executive branch entity receives Federal information only incidental to providing a service or product to the Government other than processing services, its information systems are not considered Federal Information Systems
The Impact of Federal Protected Information Regulations on Higher Education Institutions

NIST Special Publication 800-171

- 14 Security Requirement Topics (families)
  - Access control (22 controls)
  - Awareness training (3 controls)
  - Audit & Accountability (9 controls)
  - Configuration Management (9 controls)
  - Identification and Authentication (11 controls)
  - Incidence Response (3 controls)
  - Maintenance (6 controls)
  - Media Protection (9 controls)
The Impact of Federal Protected Information Regulations on Higher Education Institutions

NIST Special Publication 800-171

- 14 Security Requirement Topics (families)
  - Personnel Security (2 controls)
  - Physical Protection (6 controls)
  - Risk Assessment (3 controls)
  - Security Assessment (3 controls)
  - System & Communications Protection (16 controls)
  - System & Information Integrity (7 controls)

- Total Security Controls = 110
The Impact of Federal Protected Information Regulations on Higher Education Institutions

<table>
<thead>
<tr>
<th>CUI SECURITY REQUIREMENTS</th>
<th>NIST SP 800-53 Relevant Security Controls</th>
<th>ISO/IEC 27001 Relevant Security Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1.4 Separate the duties of individuals to reduce the risk of malicious activity without collusion.</td>
<td>AC-5 Separation of Duties</td>
<td>A.8.1.2 Segregation of duties</td>
</tr>
<tr>
<td>9.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.</td>
<td>AC-6 Least Privilege</td>
<td>A.8.1.2 Access to networks and network services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.2.3 Management of privileged access rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.4 Secure privileged use of privileged utility programs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.6 Access control to program source code</td>
</tr>
<tr>
<td></td>
<td>AC-40 Least Privilege Authorizing Access to Security functions</td>
<td>No direct mapping</td>
</tr>
<tr>
<td></td>
<td>AC-40 Least Privilege Privileged Accounts</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>9.1.6 Use non-privileged accounts or roles when accessing nonsensitive functions.</td>
<td>AC-40 Least Privilege Non-privileged Access for Nonsensitive Functions</td>
<td>No direct mapping</td>
</tr>
<tr>
<td></td>
<td>AC-60 Least Privilege Authorizing Use of Privileged Functions</td>
<td>No direct mapping</td>
</tr>
<tr>
<td></td>
<td>AC-60 Least Privilege Privileged Users from Executing Privileged Functions</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>9.1.8 Limit unsuccessful login attempts</td>
<td>AC-7 Unsuccessful Login Attempts</td>
<td>A.9.4.2 Secure login procedures</td>
</tr>
<tr>
<td>9.1.9 Provide privacy and security notices consistent with applicable CUI rules.</td>
<td>AC-8 System Use Notification</td>
<td>A.9.4.2 Secure login procedures</td>
</tr>
<tr>
<td>9.1.10 Use session lock with session-expiring displays to prevent access viewing of data after period of inactivity.</td>
<td>AC-11 Session Lock</td>
<td>A.11.2.8 Unattended user equipment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.11.2.9 Clear desk and clear screen policy</td>
</tr>
<tr>
<td></td>
<td>AC-11 Session Lock</td>
<td>No direct mapping</td>
</tr>
<tr>
<td></td>
<td>AC-11 Session Lock with session-expiring displays</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>9.1.11 Terminating a user session after a defined condition.</td>
<td>AC-32 Session Termination</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>9.1.12 Monitor and control remote access sessions.</td>
<td>AC-73 Remote Access Automated Monitoring</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>9.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.</td>
<td>AC-73 Remote Access Protection of Confidentiality / Integrity using Cryptography</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>9.1.14 Route remote access via managed access control points.</td>
<td>AC-73 Remote Access Managed Access Control Points</td>
<td>No direct mapping</td>
</tr>
</tbody>
</table>
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Safeguarding Covered Defense Information and Cyber Incident DFAR 252.204-7012

- Covered Defense Information (unclassified)
  - Provided to a contractor by DoD
  - Collected, developed, received, transmitted, used or stored by contractor
  - Controlled Technical Information
  - Critical Information
  - Export control
  - Other information as marked
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Adequate Security

- Contractor notify DoD CIO within 30 days of contract award, of any security requirements specified by NIST 800-171 not implemented at time of award; or

- Alternative security but equally effective security measures accepted in writing by an authorized DOD CIO representative.
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Adequate Security

- Cyber incident reporting requirement
  - Conduct a review for evidence of compromise of CDI
    - Identify compromised computers
    - Identify compromised servers
    - Identify compromised data and user accounts
    - Identify contractor network(s)
  - Cyber incident report
    - Medium assurance certificate
- Subcontract flow down requirements
The Impact of Federal Protected Information Regulations on Higher Education Institutions

Summary

- Controlled Unclassified Information (CUI) requires strict information technology guidelines and controls that may be in effect under fundamental research projects.
- NIST SP 800-171 outlines 110 information system controls that require a global approach.
- Covered Defense Information (CDI) requires strict guidelines and Contracting Officer approval before using CDI.
Comments or Questions

Doug Backman
University of Central Florida
dbackman@ucf.edu
(407) 882-1168