The Impact of Recent Export Control Regulations on Higher Education Institutions

Doug Backman
University of Central Florida
The Impact of Recent Export Control 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 Recent Export Control Regulations on Higher Education Institutions

Agenda

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

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

- Controlled Unclassified Information (CUI)
The Impact of Recent Export Control 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
  - Critical Information
  - Export control
  - Other information as marked
The Impact of Recent Export Control Regulations on Higher Education Institutions

Adequate Security

- Implement information systems security protections on all covered contractor information systems
  - NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  - No later than December 31, 2017
The Impact of Recent Export Control 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 Recent Export Control 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 Recent Export Control Regulations on Higher Education Institutions

NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUSSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
http://dx.doi.org/10.6027/SP.800-171
The Impact of Recent Export Control 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 Recent Export Control 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 Recent Export Control 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>3.1.4 Separate the duties of individuals to reduce the risk of inadvertent activity without collusion.</td>
<td>AC-5 Separation of Duties</td>
<td>A.6.1.2 Segregation of duties</td>
</tr>
<tr>
<td>3.1.5 Employ the principle of least privilege, including for specific, security functions and privileged accounts.</td>
<td>AC-6 Least Privilege</td>
<td>A.9.1.2 Access to networks and networked systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.3.3 Management of privileged access rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.4.4 Use of privileged utility programs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A.9.4.5 Access control to program source code</td>
</tr>
<tr>
<td></td>
<td>AC-6(a) Least Privilege Authorize Access to Security Functions</td>
<td>No direct mapping</td>
</tr>
<tr>
<td></td>
<td>AC-6(b) Least Privilege Manage Access</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.</td>
<td>AC-6(c) Least Privilege Non-Privileged Access for Nonsecurity Functions</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>3.1.7 Prevent non-privileged user from executing privileged functions and audit the execution of such functions.</td>
<td>AC-6(d) Least Privilege Auditing Use of Privileged Functions</td>
<td>No direct mapping</td>
</tr>
<tr>
<td></td>
<td>AC-6(e) Least Privilege Monitor Non-Privileged User Non-Privileged Functions</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>3.1.8 Limit unsuccessful login attempts.</td>
<td>AC-7 Unsuccessful Login Attempts</td>
<td>A.9.4.3 Secure login procedures</td>
</tr>
<tr>
<td>3.1.9 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>3.1.10 Use session lock with pattern matching and/or 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, logging out</td>
</tr>
<tr>
<td></td>
<td>AC-11(a) Session Lock Preventing Access</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>3.1.11 Terminate (automatically) a user session after a defined period.</td>
<td>AC-12 Session Termination</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>3.1.12 Monitor and control remote access sessions.</td>
<td>AC-13(a) Remote Access Automated Monitoring / Logging</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>3.1.13 Employ cryptographic means to protect the confidentiality of remote access sessions.</td>
<td>AC-13(b) Remote Access Protection of Confidentiality / Integrity / Authentication</td>
<td>No direct mapping</td>
</tr>
<tr>
<td>3.1.14 Manage remote access via remote access control policies</td>
<td>AC-13(c) Remote Access Managed Access Control Policies</td>
<td>No direct mapping</td>
</tr>
</tbody>
</table>
The Impact of Recent Export Control Regulations on Higher Education Institutions

UCF’s Case

- Cloud storage & e-mail review
- Academic & research units review
- University Information Technology support
- University budget support
The Impact of Recent Export Control Regulations on Higher Education Institutions

Controlled Unclassified Information (CUI)

- **Definition**

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 or permits an agency to handle using safeguarding or dissemination controls.

CUI does not include classified information.
The Impact of Recent Export Control Regulations on Higher Education Institutions

- CUI - Safeguarding and Dissemination

Agencies may require controls in 3 ways:

1) CUI Basic – agencies must control or protect the information with no specific controls

2) CUI Specified – agencies must provide specific controls to protect the data

3) CUI non-Specified – agencies provide some of the controls and specify only some of the controls.
The Impact of Recent Export Control Regulations on Higher Education Institutions

CUI - Safeguarding and Dissemination

- Controls – are safeguarding or disseminating controls that a law, regulation or Government-wide policy requires or permits agencies to use when handling CUI

- CUI Registry

- CUI categories and Subcategories
The Impact of Recent Export Control 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 Recent Export Control Regulations on Higher Education Institutions

- Information systems that process, store, or transmit CUI
  - Non-Federal information systems are required to follow NIST SP 800-171 requirements
The Impact of Recent Export Control Regulations on Higher Education Institutions

Summary

- Covered Defense Information (CDI) requires strict guidelines and Contracting Officer approval before using CDI
- Controlled Unclassified Information (CUI) requires strict 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
Comments or Questions

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