Controlled Unclassified Information and NIST 800-171

Trey Breckenridge

Director, High Performance Computing

Mississippi State University

MISSISSIPPI STATE UNIVERSITY™

HPC² High Performance Computing COLLABORATORY

What is Controlled Unclassified Information (CUI)?

Any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

What is NIST 800-171

- National Institute of Standards and Technology Special Publication that specifies information security standards and guidelines for Protecting **Controlled Unclassified Information** in **Non-federal Information Systems and Organizations**.
- Is intended for use by federal agencies when agencies are **providing CUI to non-federal organization** (or when **CUI is developed** by those organizations **for federal agencies**) for purposes **unrelated to information processing** (not operating their information systems to process agency data, including CUI, on behalf of the agency but rather for other purposes)
  - The purpose is to safeguard sensitive information from cyber incidents, and any consequences associated with the loss of this information are assessed and minimized via incident reporting and damage assessment.
- The requirements apply only to components of non-federal information systems that **process, store, or transmit CUI, or provide security protection** for such components.

When are these controls required?

- Contractual agreement directly references NIST 800-171.
- Contract after August 26, 2015 has DFARS 252.204-7012 clause.
- Data Sharing Agreement or Confidential Disclosure Agreement references security requirements in NIST 800-171.

Why should you care?

- How to protect the data:
  - Before: You 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 **could** require additional personnel or other resources to meet.
- If the requirements cannot be met, the university cannot enter into the contractual agreement for the grant/contract
  - End results: the loss of research funds or information necessary for university operations.

When will we see the requirements?

- NIST 800-171 originally published in June 2015
  - Updated Jan 14, 2016
  - Superseded by Rev 1, issued on December 2016
  - New revision expected on Dec 20, 2017
- DFARS 252.204-7012 modified to require NIST 800-171 on August 26, 2015 (this is a contract clause on Department of Defense Contracts).
  - NIST 800-171 compliance **required** by December 31, 2017.
- FAR Clause expected to include NIST 800-171 in 2017
  - this will impact **all** federal contracts.
- May be directly referenced in federal contracts **prior to FAR Clause**.

What type of information is categorized as CUI?

National Archives and Records Administration (NARA) has defined 22 main categories where information could be categorized as CUI:

Agriculture	Controlled Technical Information	Copyright	Critical Infrastructure
Emergency Management	Export Control	Financial	Foreign Government Information
Geodetic Product Information	Information Systems Vulnerability Information	Intelligence	Law Enforcement
Legal	NATO	Nuclear	Patent
Privacy	Proprietary Business Information	SAFETY Act Information	Statistical
Tax	Transportation		

What type of information is categorized as CUI? Potential areas of impact to MSU

Agriculture: Information related to the agricultural operation, farming or conservation practices, or the actual land of an agricultural producer or landowner.

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. Examples 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.

Copyright: Includes both published and unpublished works.

Critical Infrastructure: Ammonium nitrate; water assessments

Export Control: EAR & ITAR information

What type of information is categorized as CUI? Potential areas of impact to MSU (cont.)

Foreign Government Information: Information provided by, otherwise made available by, or produced in cooperation with a foreign government or international organization.

Geodetic Product Information: Related to imagery, imagery intelligence, or geospatial information.

Immigration: Related to admission of non-US citizens into the United States and application for temporary and permanent residency.

Law Enforcement: Related to techniques and procedures for law enforcement operations, investigations, prosecution, or enforcement actions.

Patent: Application, Invention, Secrecy orders

Privacy: Genetic Information, Health Information, Inspector General, Military, Personnel, Student Records (basically PII)

What type of information is categorized as CUI? Potential areas of impact to MSU (cont.)

Proprietary Business Information: Small Business Research and Technology; material and information related 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.

Statistical: Census, Investment Survey

Transportation: Sensitive Security Information, related to any mode of travel or conveyance by air, land, or waterway.

What are the requirements of NIST 800-171?

- 110 Individual Controls
- In the typical university environment:
  - 20% of the controls have a high difficulty factor to implement.
  - 65% of the controls have a medium difficulty factor to implement.
  - 15% of the controls are already being met or require minimal changes from existing operations.
- **All 110 controls are requirements, unless exceptions are granted by the federal agency providing oversight.**

Implementation Challenges

ACCESS CONTROL

- Separation of duties of individuals
- Employ principle of least privilege
- Monitor and control remote access sessions
- Control connection of mobile devices
- Encrypt CUI on mobile devices
- Verify and control/limit connections to and use of external systems
- Limit use of portable storage devices on external systems

Implementation Challenges (cont.)

AUDIT AND ACCOUNTABILITY

- 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
- Correlate audit review, analysis, and reporting processes
- Limit management of audit functionality to a subset of privileged users

CONFIGURATION MANAGEMENT

- Baseline configurations throughout lifecycle of equipment
- Track, review, approve/disapprove, and audit changes
- Control and monitor user-install software

Implementation Challenges (cont.)

IDENTIFCATION AND AUTHENTICATION

- Multi-factor authentication requirements
- Password management, include minimum password complexity and reuse

INCIDENT RESPONSE

- Establish operational incidence-handling capability

MAINTENANCE

- Control tools, techniques, mechanisms, and personnel used to conduct system maintenance

Implementation Challenges (cont.)

MEDIA PROTECTION

- Control the user of removable media on system components
- Prohibit the user of portable storage devices when such devices have no identifiable owner

PERSONNEL SECURITY

- Ensure protection of CUI during personnel actions such as terminations and transfers

PHYSICAL PROTECTION

- Escort visitors and monitor visitor activity
- Maintain audit logs of physical access

Implementation Challenges (cont.)

RISK ASSESSMENT

- Periodically assess and document risk to operations, assets, and individuals

SECURITY ASSESSMENT

- Develop, document, and periodically update system security plans

SYSTEM AND COMMUNICATIONS PROTECTION

- Prevent unauthorized and unintended information transfer via shared system resources
- Separate publicly accessible systems from internal networks
- Deny communications traffic by default and allow traffic by exception
- Control and monitor the use of mobile code
- Prohibit remote activation of collaborative computing devices

Implementation Challenges (cont.)

SYSTEM AND INFORMATION INTEGRITY

- Identify, report, and correct information and system flaws in a timely manner
- Provide protection from malicious code
- Monitor systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks
- Identify unauthorized use of the systems