Student Data and Controlled Unclassified Information (CUI)

K-State Stance and Action Plan
Dr. Gary Pratt & Chad Currier
Controlled Unclassified Information (CUI)

Information provided by, collected, or maintained on behalf of, the executive branch of the United States government, and aligns with at least one of the CUI Registry categories.

Executive Order 13556

- Order establishes a program for managing CUI that emphasizes the openness and uniformity of Government-wide practice
- Established on 11/4/2010 under the 44th Administration

CUI Registry examples

- Export Control
- Intelligence
  - Agriculture
- Natural and Cultural Resources
- Nuclear
- Privacy
  - Student Records
- Transportation
Controlled Unclassified Information (CUI) – Student Records

https://www.archives.gov/cui/registry/category-detail/student-records
What is NIST 800-171

- NIST Special Publication 800-171 defines the security requirements (controls) required to protect CUI in nonfederal information systems and organizations.
- Information systems that process, store, or transmit CUI may be federal or nonfederal.
- It contains 110 controls across 14 control families.
- Controls divided into Security Requirement Families:

<table>
<thead>
<tr>
<th>FAMILY</th>
<th>FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Media Protection</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Physical Protection</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Identification and</td>
<td>Security Assessment</td>
</tr>
<tr>
<td>Authentication</td>
<td>System and Communications</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Protection</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System and Information Integrity</td>
</tr>
</tbody>
</table>
Current Environment

- Student Data has been marked as CUI
- Compliance with this standard is in accordance with 32 C.F.R Part 2002
- FSA Self-assessment initiative was to launch in 2021 – No update
- The Student Aid Internet Gateway (SAIG) Enrollment Agreement entered into by each Title IV-participating institution includes a provision that the institution “[m]ust ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel.”
  - institutions may be responsible for losses, fines, and penalties (including criminal penalties) as a result of data breaches.
- Systems containing student data are everywhere
- Discovery alone is a challenge
- These changes are disruptive
- Balance is key: Academic Freedom WILL be impacted, we need to ensure buy-in.
- K-State is not stopping
  - This is not and cannot be an IT problem, this is an institution problem.
K-State – Plan of Action

Cross-Functional Teams

• Project Governance Group
  – Pushing back on shadow systems

• Data Governance Group
  – Identify and register student data
  – Identify appropriate data custodian(s)
  – Buy-in and evangelism

• Data & Cyber Security Compliance Group
  – Singular focus is CUI and student data – Led by AVP for Risk and Compliance – Not IT
  – Tasked with discovery, education, policy
  – Representation: Audit, IT, Registrar, Financial Aid, Research, Records Management, Risk and Compliance

Division of IT

• Policy push – lengthy process at KSU

• Discovery

• Cyber Risk Assessment Team – Established
  – GLBA
  – CUI
  – K-State Internal Audit

• Environment Preparation
  – AWS – NIST 800-53 Technical controls
  – Azure – RISE CUI
  – Internal Data Center

• Working with Research and external consultants – Gap Analysis
<table>
<thead>
<tr>
<th>Access Control</th>
<th>Control Number</th>
<th>Control Description</th>
<th>Equivalent Control AC-5-2</th>
<th>AC-11-19</th>
<th>AC-11-19</th>
<th>AC-11-19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>3.1.1</td>
<td>Empower perpetual</td>
<td>Access Control Operations</td>
<td>3.1.2</td>
<td>3.1.2</td>
<td>3.1.2</td>
</tr>
<tr>
<td>Access Control</td>
<td>3.1.2</td>
<td>Limit system access</td>
<td>to the terms of</td>
<td>Allocation, function</td>
<td>process, function</td>
<td>of allocation, function</td>
</tr>
</tbody>
</table>

**K-State – Gap Analysis -- RISE**

- Current view is into RISE – Research Enclave
- Will conduct this exercise into AWS and On-Prem
- Tool for Internal Audit and Risk Assessment teams on shadow systems
NIST 800-171– Phase I
Approach to Compliance

• Compliance Group established to focus on CUI implementation on admin function of the University
• Review on the impact of CUI controls on admin operation
• NIST 800-171 training
• Presentation to get President’s Cabinet approval and buy-in
• Create sub-groups for physical controls and policy writing
NIST 800-171– Phase II

Policy and Process

• Convene policy task force and provide charge/timeline
• Convene physical task force and provide charge/timeline
• Policy task force reports progress on policy and process to core group
NIST 800-171 – Phase III

Self Assessment

• Tier I systems
  – 110 controls self-assessment
  – Updates to policy reported to policy task force
  – Reports compliance to core group

• Tier II systems – work begins after Tier I completed
  – 110 controls self-assessment
  – Updates to policy reported to policy task force
  – Reports compliance to core group

• Shadow Systems – Continual effort
  – Identification of systems continues – Some will be recommended for decommission
    • 110 controls self-assessment
    • Updates to policy reported to policy task force
    • Reports compliance to core group
NIST 800-171– Phase IV

Conclude and Monitor

- Sub-group meets to review compliance and assess remaining gaps
- Sub-group receives task force report of completed work, reviews, and determines next review.
Helpful Sites:

• https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf
• https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
• https://er.educause.edu/articles/2021/3/800-171-compliance-on-the-horizon