Agenda

- **Practical steps to comply with NIST 800-171** and requirements for Controlled Unclassified Information (CUI)
- Understanding the requirements, and **what they mean in practice**
- Using your CUI program to **take your campus to the next level on data security**
Controlled Unclassified Information (CUI)

**What is Controlled Unclassified Information?**
CUI can be any data received from the federal government that is not designated as classified; this can include but is not limited to:

- Controlled technical information
- Patent information
- Export control data
- Research data
- Engineering data and drawings
- Agricultural data
- Privacy data
- Health records
- Financial information (i.e. student loans)
- Student records
- Genetic Data

**What is being required?**
NIST SP 800-171 has been designated by the US Government as the minimum security standard for protecting CUI data associated with federal contracts.

US Government agencies are being required to consolidate and transform over 100 different policies and markings to comply with CUI Program requirements, involving an estimated $25 billion in higher education research contracts and grants alone.

**What does this mean for higher educational institutions?**
Traditional approaches to cybersecurity are no longer adequate. While many contractors already deal with a great many government regulations and reporting requirements, NIST 800-171 demands special attention. Organizations that do not comply risk losing federal funding for research and, potentially, financial aid.

---

**A roadmap to CUI compliance**

1. **Analyze** the impact and scope
2. **Access** the current state of security
3. **Develop a plan** to achieve compliance and mitigate existing gaps
4. **Establish responsibilities and efficient processes** to achieve sustained compliance over the long haul
5. Employ third-parties as needed to provide a thorough review of current practices across the entire academic enterprise

**A path to compliance:**
Form a working group with representatives from academics, administration, and research; the group should have top-down support and the sustained engagement of leadership.

Once formed the working group should consider the following.
Overcoming top challenges
Compliance with the spirit of NIST 800-171 goes well beyond technological solutions.

1. **Executive and board-level attention:**
   - This is not yet on the radar of many institutional leaders or boards of trustees.
   - Reframe in terms of enterprise risk management, with the business impact to the institution clearly spelled out.

2. **Cultural barriers:**
   - Colleges and universities have often enjoyed a culture of openness and sharing.
   - Stress the need for enhanced security while maintaining a federated model for data sharing and access.

3. **An enterprise-level solution** is needed, as is a central authority to assess and certify data and access compliance.

**IT operating model**
Factors to consider to enhance the IT operating model of an institution

<table>
<thead>
<tr>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What services are provided in the current IT operating model?</td>
</tr>
<tr>
<td>• Should existing services change?</td>
</tr>
<tr>
<td>• What processes need to be added / modified / eliminated?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What underlying technologies should be used to deliver services in the IT operating model (e.g., ERP, CRM, self-service)?</td>
</tr>
<tr>
<td>• What should the application architecture look like (e.g., how do new or changing systems fit in with the technology landscape)?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• How many physical locations are required in an optimized IT operating model?</td>
</tr>
<tr>
<td>• Where will staff be located?</td>
</tr>
<tr>
<td>• What are the space and facility requirements?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>• How should faculty, staff and students interact and work with the operating model?</td>
</tr>
<tr>
<td>• What channels of interaction should be supported (e.g., phone, email, web, walk-up, etc.)?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Who is providing services in the IT operating model?</td>
</tr>
<tr>
<td>• Are changes needed in organizational units and teams to provided needed services?</td>
</tr>
<tr>
<td>• How many people are needed to provide services?</td>
</tr>
</tbody>
</table>
Lessons learned from other industries

By leveraging these overarching themes from the aerospace and defense industry, higher education institutions can build a strong CUI foundation.

Data categorization
Data should be categorized as an institution. This is the foundation of a successful CUI implementation. Without correctly categorizing data, costs will likely increase through different uses of technology solutions and policies could be applied to incorrect data sets.

Leverage existing technology
Many technology systems already in place at an institution have the capabilities to address CUI requirements. The key is understanding who the technology reaches and which data it houses.

Write overarching policies
Overarching policies can encompass CUI, along with other regulatory requirements. This allows organizations to be nimble while conducting operations in a changing regulatory environment.

Case Study
Large Multi-Member University System
"Protecting our University’s research data is of great importance to the Texas A&M System’s Research Security Office. We take a holistic approach to protecting the confidentiality of CUI and ensure our researchers have a secure environment to do what they do best."

Dr. Kevin R. Gamache, Chief Research Security Officer
The A&M System Research Security Office (RSO)
The RSO helps A&M System Principal Investigators (PIs) maintain federal funding for research by meeting requirements for safeguarding Controlled Unclassified Information (CUI) and other federal information.

**RSO Mission:** Establish and administer research security policies, procedures and technology to enable Texas A&M University System Members to comply with Federal guidelines for handling all levels of U.S. Government information.

**IT Operations**
- Secure Computing Enclave (SCE) Help Desk
- Network and infrastructure engineering and maintenance
- Account management

**Security Operations**
- Vulnerability scanning
- Penetration testing
- Antivirus management
- Multi-factor authentication and PKI management
- Facilities security coordination

**Research Security Support & Compliance**
- A&M System relations
- Government liaison
- Regulatory compliance monitoring
- Training and awareness activities
- Audit readiness activities

The RSO reduces the burden of compliance for PIs by enabling the security of regulated research data through the management of the RSO’s SCE and the administration of necessary policies.

RSO Stakeholder Engagement
The RSO focused on six primary communities for engagement during design work. PIs received the highest level of engagement via the Council of Principal Investigators (CPI).

<table>
<thead>
<tr>
<th>Community</th>
<th>Leadership</th>
<th>Community-Specific Engagement Activities</th>
<th>Future State Engagement Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIs and Researchers</td>
<td>CPI, other bodies as appropriate</td>
<td>• Proactive communications on upcoming issues&lt;br&gt;• Continuous support regarding inquiries&lt;br&gt;• Regular CPI meetings to gather feedback&lt;br&gt;• Interviews to understand research needs</td>
<td>• All-Hands Meetings, keeping all stakeholders involved with the RSO up-to-date and in sync</td>
</tr>
<tr>
<td>IT Admin.</td>
<td>Member Chief Information Officers (CIOs)</td>
<td>• Initial meetings with IT groups regarding RSO technical performance, capability gaps, high priority risks and shared services (e.g. SOC and single sign-on)</td>
<td>• Periodic communications informing all stakeholders of recent events regarding RSO performance and security support</td>
</tr>
<tr>
<td>Research Admin.</td>
<td>Member Chief Research Officers (CROs)</td>
<td>• Initial meetings with research administrators regarding security issues impacting PI communities within the A&amp;M System</td>
<td>• Standing meetings for the most critical groups, especially those that support a service provided by the RSO</td>
</tr>
<tr>
<td>Compliance Officers</td>
<td>System Compliance Officer, General Council (GC)</td>
<td>• Initial meetings with A&amp;M System VP of Compliance and GC regarding audit readiness</td>
<td>• In person meetings or presentations to utilize existing channels or for difficult topics</td>
</tr>
<tr>
<td>Academic Admin.</td>
<td>Member Chief Academic Officers (CAOs)</td>
<td>• Planned meetings with CAOs to coordinate academic initiatives with RSO operations</td>
<td>• Feedback channels allowing continual input from communities</td>
</tr>
<tr>
<td>System Support Services</td>
<td>Heads of Service Areas</td>
<td>• Collaboration on the support of in-scope PI contracts for federal research&lt;br&gt;• Interactions to agree on shared services and responsibilities for involved parties</td>
<td></td>
</tr>
</tbody>
</table>
A persona representing a "typical" PI helped the RSO better understand their audience, guiding design decisions.

**PI Persona**

**Dr. Nguyen**

*Role:* Principal Investigator

*Faculty:* 10 years

*Degree:* Accredited Engineer, Informational Security

*Institution:* Current IT System

*Job Description:* Cybersecurity

**What is my work like?**

I’ve worked on projects of various kinds. From Ike’s budgets cut a throughput by a number of millions that year-was. Government research systems like working on it, so I'm trying to continue with it.

The technology or equipment used in my projects varies. The more projects I do in the future, the better. At times, I had my own equipment in certain systems I had specific needs. Some PIs might go into a room where they can see federal or state espionage, with which we’re collaborating. The research needs are different, but should be able to be sourced from other personnel if needed.

Cybersecurity hasn’t been a major concern for my projects—I do. The System should be worried about them. Also, when new is involved, the contract office (OC) asked a colleague or involved in a grad student.

**What are my motivations and frustrations?**

**MY MOTIVATIONS**

Moving forward, my work is in my identity. I’m recognized in my field by the type of work I do, and my ability to add value to things. I enjoy the complex and challenging problems that arise. 

We’re dealing with a more innovative world. I’m interested in the work itself, and in helping others understand the science. I’m making a meaningful contribution to knowledge and doing good. At the same time, I’m still taking on new challenges.

**Understanding Cybersecurity:**

Cybersecurity is not a science. It’s an art. We’re dealing with a more innovative world. We’re dealing with a more innovative world. 

As a cybersecurity, my staff has other responsibilities. I need to focus on and I’ve never had a breach. Which is the norm, it’s worrying about it now? Not a, it seems problematic in the academic and government I worked. 

If there’s no data at-risk funding for me or my research and we suffer the reputational damage that would be associated with a compromised breach at some point in the future. I’d like to find a way to deal with it. (CI) 

---

**Federal Information Security Compliance: Current State**

The A&M System has achieved initial DFARS compliance with input from PIs and assistance from Deloitte. This effort requires additional action and should produce clear benefits.
Deloitte Support Overview

Deloitte helped to establish the RSO and design a secure computing enclave to enhance information security and reach initial compliance ahead of the DFARS deadline.

Deloitte assisted the A&M System in three primary areas:

<table>
<thead>
<tr>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Design</td>
<td>Policies and Procedures</td>
<td>Architecture</td>
</tr>
<tr>
<td>• Operating Model</td>
<td>• IT Security Standards &amp; Procedures</td>
<td>• Architectural Blueprint Design Document</td>
</tr>
<tr>
<td>• Organizational Chart</td>
<td>• IT Operations Standards &amp; Procedures</td>
<td>• RSO Bill of Materials (BCM)</td>
</tr>
<tr>
<td>• Role Mapping</td>
<td>• Compliance and Audit Artifacts</td>
<td>• RSO Cost Model</td>
</tr>
<tr>
<td>• Job Descriptions</td>
<td>• Security Traceability Matrix (STM)</td>
<td>Core Services and Application Hardening</td>
</tr>
<tr>
<td>Organizational Change Management</td>
<td>• System Security Plan (SSP)</td>
<td>• Hardening Guides</td>
</tr>
<tr>
<td>• Organizational Change Strategy</td>
<td>• Plans of Action and Milestones (POAMs)</td>
<td>• Hardening Narrative &amp; Presentation</td>
</tr>
<tr>
<td>• Stakeholder Engagement</td>
<td>Data and Personnel Lifecycle Management</td>
<td>Data and Personnel Lifecycle Management Documentation</td>
</tr>
</tbody>
</table>

These activities have set the foundation and established a roadmap for the RSO and the secure computing enclave to safeguard systems for federal research.

Department of Education

"The Department understands the investment and effort required by institutions to meet and maintain the security standards established under NIST SP 800-171. Nonetheless, across the public and private sectors, it is imperative that organizations continue to enhance cybersecurity in order to meet evolving threats to CUI and challenges to the security of such organizations. Thus, we strongly encourage those institutions that fall short of NIST standards to assess their current gaps and immediately begin to design and implement plans in order to close those gaps using the NIST standards as a model."

Questions

Kenneth J. Liddle
Chief Compliance Officer
Rice University
kliddle@rice.edu

Kevin R. Gamache, Ph.D.
Chief Research Security Officer
The Texas A&M University System
krgamache@tamus.edu

Justin Williams
Cyber Risk Executive
Deloitte
jmwilliams@deloitte.com

Other resources:

NIST Special Publication 800-171 for higher education
A guide to helping colleges and universities comply with new federal regulations.