



Kenneth Liddle, Chief Compliance Officer, Rice University
Kevin R. Gamache, Ph.D., Chief Research Security Officer, The Texas A&M University System
Justin Williams, Cyber Risk Executive, Deloitte

Controlled Unclassified Information (CUI)
June 2019

1

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**

2

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

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.**

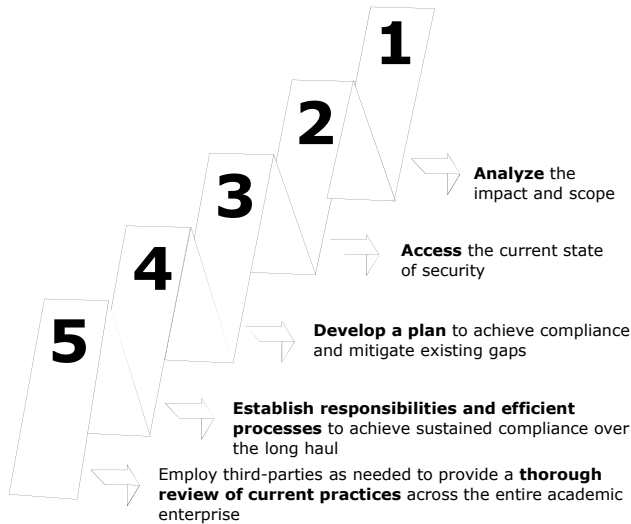
Organizations that do not comply risk losing federal funding for research and, potentially, financial aid.

Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

3

A roadmap to CUI compliance



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.

Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

4

Overcoming top challenges

Compliance with the spirit of NIST 800-171 goes well beyond technological solutions.



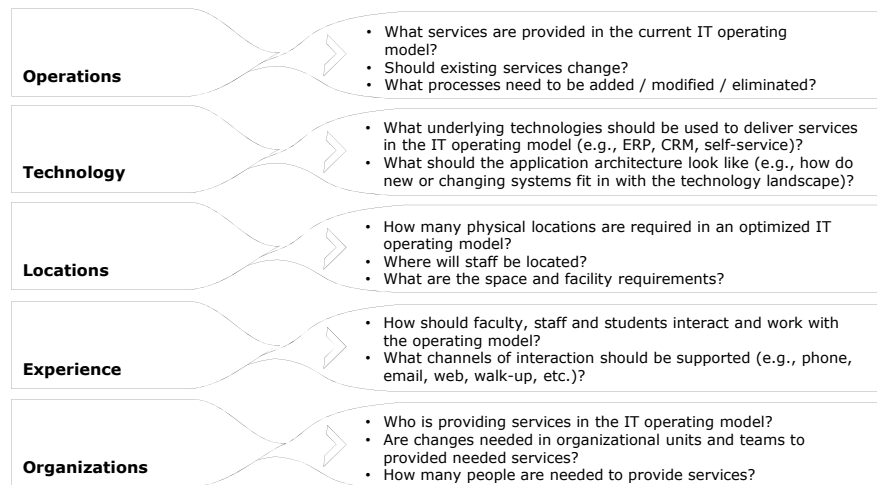
Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

5

IT operating model

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



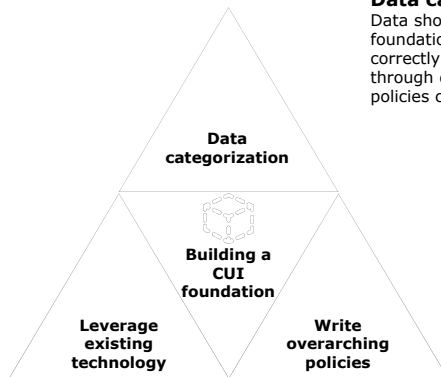
Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

6

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.

Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

7

Case Study

Large Multi-Member University System

8

Defense Security Service

Award for Excellence in Counterintelligence

James S. Cogswell

Award for Industrial Security Excellence

The Texas A&M University System

9

*"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.**"*

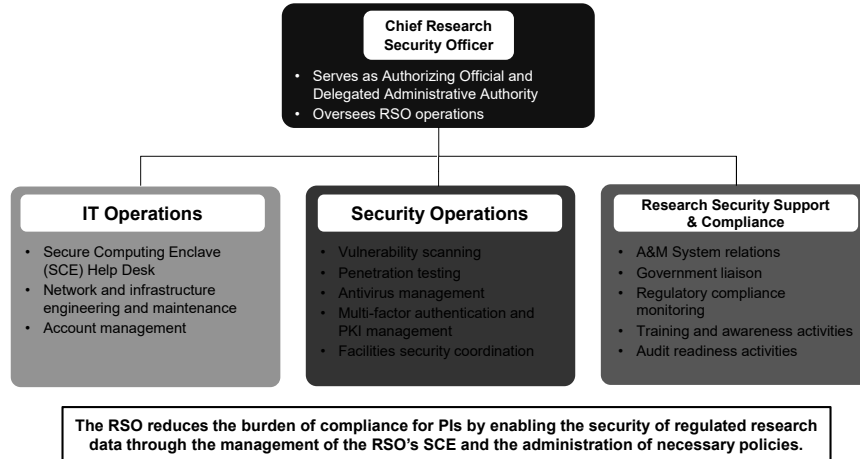
Dr. Kevin R. Gamache, Chief Research Security Officer

10

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 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.



Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

11

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).

Community	Leadership	Community-Specific Engagement Activities	Future State Engagement Activities
PIs and Researchers	CPI, other bodies as appropriate	<ul style="list-style-type: none"> Proactive communications on upcoming issues Continuous support regarding inquiries Regular CPI meetings to gather feedback Interviews to understand research needs 	<ul style="list-style-type: none"> All-Hands Meetings, keeping all stakeholders involved with the RSO up-to-date and in sync Periodic communications informing all stakeholders of recent events regarding RSO performance and security support Standing meetings for the most critical groups, especially those that support a service provided by the RSO In person meetings or presentations to utilize existing channels or for difficult topics Feedback channels allowing continual input from communities
IT Admin.	Member Chief Information Officers (CIOs)	<ul style="list-style-type: none"> Initial meetings with IT groups regarding RSO technical performance, capability gaps, high priority risks and shared services (e.g. SOC and single sign-on) 	
Research Admin.	Member Chief Research Officers (CROs)	<ul style="list-style-type: none"> Initial meetings with research administrators regarding security issues impacting PI communities within the A&M System 	
Compliance Officers	System Compliance Officer, General Council (GC)	<ul style="list-style-type: none"> Initial meetings with A&M System VP of Compliance and GC regarding audit readiness 	
Academic Admin.	Member Chief Academic Officers (CAOs)	<ul style="list-style-type: none"> Planned meetings with CAOs to coordinate academic initiatives with RSO operations 	
System Support Services	Heads of Service Areas	<ul style="list-style-type: none"> Collaboration on the support of in-scope PI contracts for federal research Interactions to agree on shared services and responsibilities for involved parties 	

Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

12

PI Persona

A persona representing a "typical" PI helped the RSO better understand their audience, guiding design decisions.

Dr. Nguyen
 Role: Principal Investigator
 Faculty: 15 years
 Details: Accomplished Engineer, International Background

Satisfaction: Current IT Systems
 Low High

Self-Direction
 Low High

Collaboration Needs
 Low High

Faculty Workload
 Low High

Relationship: Administration
 Cold Warm

Understanding: Cybersecurity
 Low High

Understanding: Security Reqs.
 Low High

"I'm focused on my research, my students and my career. Administration should be working hard to get anything out of the way that impedes progress, slows me down, or impacts my budget."

What is my work like?

I've worked on projects of various sizes, from \$1k budgets over a short term to budgets of millions that span years. Government research seems to be working for me, so I intend to continue with it.

The technology or equipment I use in my projects varies. The more access I have to what I need, the better. At times, I've built my own equipment or used custom software to meet specific needs. Some PIs must go to other schools to access equipment because of security requirements, which is frustrating. I like remote access to everything, but I should be able to access equipment in person if I want.

Cybersecurity hasn't been a major concern for my projects – the System should be worrying about that. But, when I've had a need, I've contacted my ISO, asked a colleague or handed it to a grad student.

My (Engineering) Research Process

What are my motivations and frustrations?

MY MOTIVATIONS
 My research, my work is my identity. I'm recognized in my field by the type of work I pursue and my ability to publish new insights. I enjoy the process and challenge of discovery while I help advance the state of the science. I'm making a meaningful contribution to knowledge and doing good. At the same time, I'm building a legacy through the next generation of researchers. Occasionally, I've seen my research commercialized and applied more broadly. That can be satisfying too.

I set the direction for my research interests and methods. While it's useful to be associated with Texas A&M, I secure the funding, I bear the burden of success, and I lead the research – when it's worth doing, I get it done. So, it's very reasonable that Administration should strive to support my work.

Conducting research is a collaborative effort. My team and I share data via whatever platform works best – external or portable media, Dropbox, email, projectors in meetings and other methods. My research team is composed of individuals of various abilities, from students to full time staff. At times I have subcontractors and other PIs collaborate.

MY FRUSTRATIONS
 Administration often seems disconnected from the needs of faculty and students. Politics and new policies impact my work processes, then I'm required to take training I don't need or my administrative burden increases. This takes away time and energy from better pursuits and impedes the mission of Texas A&M. Now I'm doing more than I ever have and not all of it is beneficial. So in the end, I'm going to choose what's most worth my time.

As to cybersecurity, my staff has other responsibilities I need them to focus on and I've never had a breach – what's the rationale for worrying about it now? Further, tight security seems antithetical to the academic ideal of openness. I must be able to freely share data and findings when and how it's best – security policies will get in the way.

What are my needs regarding new regulations and compliance?

If I'm going to go along with Administration's solution to the government's new information security requirements, you should definitely help me understand what I get out of it and who is paying for it. Be sure that you're targeting the right researchers too – the security controls don't apply to everyone.

Once it's clear that you have the right PIs and how you will benefit them, I'll need to know what the standards are and what to do about them. We can start with some basic information, like what is DFARS, CD/UCI and what are the controls? From there, we could move to some actions, which should be as minimal as possible. Administration should bear the compliance burden much more than they should pass it to me.

In the past, when I've needed to deal with government compliance, I've relied on other groups such as the Compliance Office, Research Compliance or Biosecurity to take care of what they can. Government websites are occasionally helpful as well. Some of my peers have had similar issues to what I experience so they can be useful too. When I'm stretched, I may reach out to a compliance officer in the A&M System.

In the end, I have no desire to risk funding for me or my fellow researchers or suffer the reputational damage that would be associated with a cybersecurity breach so we're going to figure it out – just don't overdo it.

Copyright © 2019 Deloitte Development LLC. All rights reserved. 303 Developing a Program for Controlled Unclassified Information (CUI)

13

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.

Audit-Readiness: Complete

Governance: In Progress **Technical: In Progress**

Benefits

- Enhanced reputation:** Leading as a top-tier research institution, receiving recognition for security excellence
- Greater adoption:** Resulting from continued PI engagement
- Economies of scale:** Building on existing research information security programs
- Competitive advantage and growth:** Attracting new federal grants and new researchers
- Managed administrative burden:** PIs focus more on research
- Improved automation:** Implementing cutting edge technology to limit IT staffing needs and administrative burden on PIs

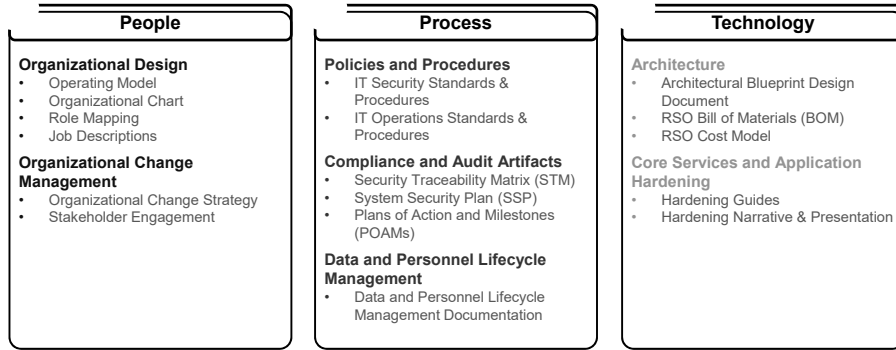
Copyright © 2019 Deloitte Development LLC. All rights reserved. 303 Developing a Program for Controlled Unclassified Information (CUI)

14

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:



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

Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

15

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."

- DCL GEN 16-12 (<https://ifap.ed.gov/dpclletters/GEN1612.html>)

Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

16

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.

Copyright © 2019 Deloitte Development LLC. All rights reserved.

303 Developing a Program for Controlled Unclassified Information (CUI)

17



Official Professional Services Sponsor

Professional Services means audit, tax, consulting and financial advisory services.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2019 Deloitte Development LLC. All rights reserved.
36 USC 220506
Member of Deloitte Touche Tohmatsu Limited

18