Deloitte.

NIST Special Publication 800-171 for Higher Education

A guide to helping colleges and universities address compliance

"The protection of Controlled Unclassified Information while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations."

— NIST Special Publication 800-171

Higher education institutions are being asked to comply with new federal rules with heightened requirements to safeguard data known as Controlled Unclassified Information (CUI). By December 31, 2017, select grants and contracts with the federal government may be subject to additional requirements, and timely compliance will be essential to avoid potential fines or the loss of contracts that could impact the institution's research and preeminence missions.

Institutions that process, store or transmit CUI data — such as student financial aid information or research conducted under federally funded contracts — may be impacted. This can include, but is not limited to:

- **Agriculture Data**
- **Controlled Technical Information**
- **Engineering Data & Drawings**
- **Export Control Data**
- **Financial Information (Student Loans)**
- **Genetic Data**
- **Health Records**
- **Patent Information**
- **Privacy Data**
- **Research Data**
- **Student Records**

Prioritizing compliance

The Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.7012 establishes the National Institute of Standards and Technology's Special Publication 800-171 (NIST SP 800-171) as the minimum security standards for protecting both CUI and Covered Defense Information (CDI) associated with defense related contracts. The Federal Acquisition Regulation (FAR) clause is also expected to apply NIST SP 800-171 standards to protect CUI associated with civilian contracts. Institutions will therefore face additional contractual requirements, likely associated with federal grants and research contracts as the National Institute of Standards and Technology's Special Publication 800-171 (NIST SP 800-171) covers 14 groups of security control families.

If organizations fail to comply with these new regulations, they risk the loss of access to mission-critical data, and consequently government funding that contributes to research and day-to-day operations. Furthermore, there's a risk of remaining non-compliant if institutions adopt the wrong technology or compliance activities. This could result in exposure to data breaches or regulatory audit findings causing brand and financial damage.

Indeed it remains unclear what the future regulatory environment will look like including general expectations, standards, and penalties. This may force higher education institutions to spend increasingly more resources and time on NIST compliance activities.

NIST SP 800-171 Security Control Families

NIST SP 800-171 groups 110 basic and derived control requirements across the following 14 families.

- Access control
- Audit and accountability
- Awareness and training
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Program management
- Risk assessment
- System and communication protection
- System and information integrity

How can Deloitte help?

While each institution will be impacted differently by the new regulations, there are critical activities that should be undertaken to manage these compliance requirements. Deloitte, the leading provider of cyber governance, can help institutions both meet their December 31, 2017 compliance requirement, as well as maintain and monitor ongoing compliance by following a methodical approach.

Deloitte's NIST SP 800-171 Solution

Methodically analyze impact and scope

Determine the applicable contracts and identify data that must be controlled

Determine value of receiving and using applicable data

Assess current state

Trace CDI/CUI through systems and processes

Develop a cross walk across any relevant/ existing compliance measures or standards used

Perform a gap analysis against NIST SP 800-171 standards

Plan for compliance and mitigate gaps

Develop a framework of controls to help address standards and compliance

Define roles and responsibilities to achieve and maintain compliance

Develop a plan of action to implement gap-fix measures with reasonable milestones

Establish/improve processes to sustain compliance

Deploy communications and training

Conduct on-going self-assessments

Undertake continuous improvement

Methodically, an institution should understand how it's impacted and whether benefits outweigh costs of compliance. If a decision is made to move forward, create an assessment of current capabilities along with a plan to comply. Lastly, define and implement long-term processes as well as roles and responsibilities to sustain compliance.

The Deloitte difference

Deloitte is a market leader in designing and deploying cybersecurity, compliance and transformational solutions. We also bring a deep understanding of higher education, based on over 90 years of serving colleges and universities, and combine that with the extensive experience in our Federal practice obtained from implementing relevant cyber security standards.

As a result, we offer an unparalleled ability to effectively interpret NIST SP 800-171 requirements and design and deploy federally compliant systems and processes that address the specific needs of our higher education clients.

Our tools, accelerators, and methodologies can help your institution:

- **engage appropriate stakeholders**
- **scope compliance efforts**
- **assess current security and controls**
- **develop plans for compliance**
- **mitigate gaps**
- **implement organization changes**
- **deploy effective communication and training**
- **implement sustainable and efficient processes for ongoing compliance**

Looking ahead

The changing regulatory landscape will require institutions to remain vigilant as they build out their NIST programs. It's important for institutions to be strategic in the adoption of compliance activities by understanding their particular set of requirements and expectations. Deloitte can help higher education institutions understand this dynamic regulatory landscape, and promptly help them achieve compliance by implementing the required compliance activities that can become sustainable and integrated with day-to-day operations. More importantly, by being strategic with their decisions, institutions can reduce overall compliance costs by choosing the requisite programs from the start.

The breadth of our capabilities across contract compliance, risk management, IT consulting and organizational transformation allows us to define an approach that can efficiently and effectively align people, process, and technology. We can help higher education institutions meet their NIST SP 800-171 compliance obligations which will be required to maintain project funding and avoid other compliance issues that may result.

Contact us:

Mark Ford
Principal
Deloitte Risk & Financial Advisory
+1 313 394 5313
mford@deloitte.com

Michael Wyatt
Principal
Deloitte and Touche LLP
+1 512 771 8062
miwyatt@deloitte.com

Richard Rudnicki
Specialist Leader
Deloitte & Touche LLP
+1 313 401 5263
rrudnicki@deloitte.com

Justin Williams
Senior Manager
Deloitte & Touche LLP
+1 346 224 5001
jmwilliams@deloitte.com

Deloitte.