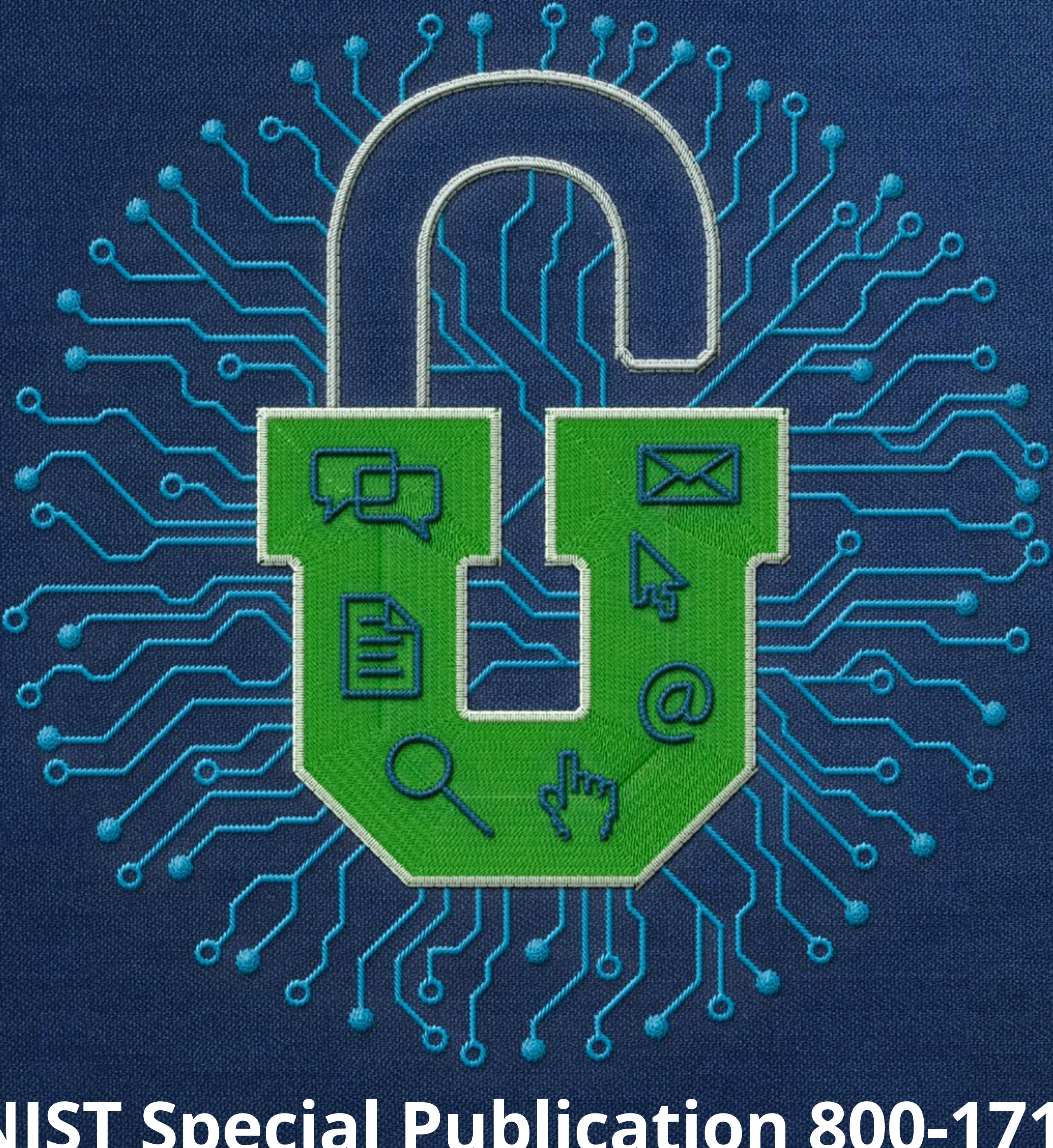
Deloitte. Insights

EDUCAUSE

A report by the Deloitte Center for Higher Education Excellence



NIST Special Publication 800-171 for higher education

A guide to helping colleges and universities comply with new federal regulations

ABOUT EDUCAUSE

EDUCAUSE (www.educause.edu) is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision-making at every level within higher education. A global nonprofit organization, EDUCAUSE members include US and international higher education institutions, corporations, not-for-profit organizations, and K-12 institutions. With a community of more than 85,000 individual participants located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. The EDUCAUSE Cybersecurity Program offers a number of resources to help colleges and universities develop and mature their information security and privacy programs.

ABOUT DELOITTE'S CENTER FOR HIGHER EDUCATION EXCELLENCE

Higher education institutions confront a number of challenges, from dramatic shifts in sources of funding resulting from broader structural changes in the economy, to demands for greater accountability at all levels, to the imperative to increase effectiveness and efficiency through the adoption of modern technology.

Deloitte's Center for Higher Education Excellence produces groundbreaking research to help colleges and universities navigate these challenges and reimagine how they achieve excellence in every aspect of the academy: teaching, learning, and research. Through forums and immersive lab sessions, we engage the higher education community collaboratively on a transformative journey, exploring critical topics, overcoming constraints, and expanding the limits of the art of the possible.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.

CYBERSECURITY FOR COLLEGES AND UNIVERSITIES

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 more than 90 years of serving colleges and universities, and combine that with the extensive experience in our Federal practice obtained from implementing relevant cybersecurity 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.

COVER IMAGE BY: ALEX NABAUM

CONTENTS

Introduction | 2

Meet NIST Special Publication 800-171 | 3

The current state: Where colleges and universities are now | 6

Getting from here to there: A road map for compliance | 8

Recommended reading | 11

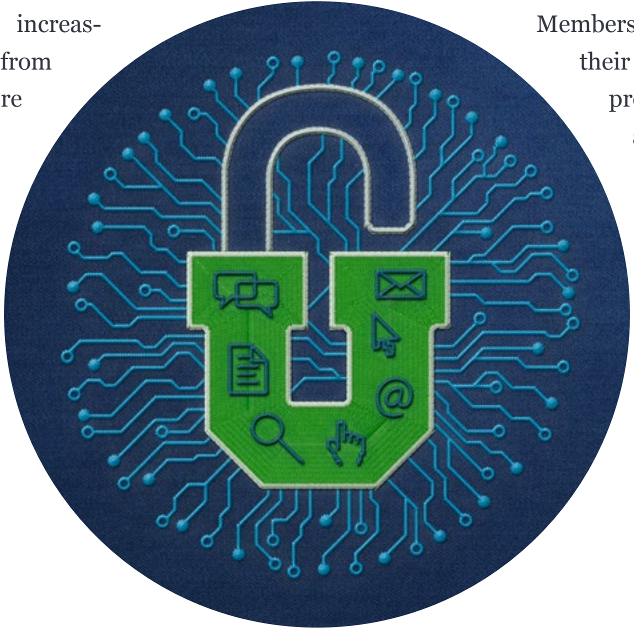
Endnotes | 12

Introduction

IN order to address increasing cyber risk and comply with new government regulations, colleges and universities that enter into contracts with federal agencies must give heightened attention to their cybersecurity measures. The last decade has seen a significant rise in the number of cyber incidents affecting federal agencies: Between fiscal years 2006 and 2015, agencies reported cyber incidents increasing over 1,300 percent, from 5,500 annually to more than 77,000.[1]

And given the volume of sensitive federal information that agencies share with third parties—including colleges and universities—the government has strengthened its requirements for safeguarding a broad set of controlled unclassified information (CUI).

In July 2017, Deloitte and EDUCAUSE convened an expert panel to discuss the implications for higher education institutions in protecting CUI received from the federal government in institutional information technology systems. Members of the panel shared their insights about CUI data protection requirements and their approaches to achieving compliance with those requirements. This article provides a high-level summary of their discussion as well as a road map for compliance activities.



Meet NIST Special Publication 800-171

FOR many leaders in institutions of higher learning, getting information security under control is about to become critical to funding and more. Whether a college or university has many large government research contracts or one small contract, it will need to comply with the requirements laid out in National Institute of Standards and Technology (NIST) Special Publication 800-171. These requirements are designed to protect the confidentiality of CUI residing in nonfederal systems. (See sidebar, "The legal basis for protecting 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
- Health records
- Financial information (on, for example, student loans)
- Student records
- Genetic data

The Defense Federal Acquisition Regulation Supplement 252.204.7012 establishes NIST 800-171 as the *minimum* security standard for protecting both CUI and covered defense information (CDI) associated with defense-related contracts. The Federal Acquisition Regulation (FAR) clause, with expected publication in late 2017, is also anticipated to apply NIST 800-171 standards to protect CUI associated across a broader set of civilian contracts.[2] Higher education institutions will face contractual requirements—most likely associated with federal grants, research contracts, and other transactions in which the institution receives data from the federal government—that will mandate compliance. In 2016, the US Department of Education communicated its intention to make student financial data subject to NIST 800-171 controls in the future and encouraged institutions to conduct a gap analysis between their current security measures and NIST 800-171 requirements.[3]

Institutions receiving defense contracts with provisions for CUI must comply by December 31, 2017. Institutions are already seeing provisions

> 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***

about the new standards inserted into defense contracts, and defense agencies are adding no-cost change orders to existing defense contracts, requiring NIST 800-171 compliance. For all others, the FAR clause may publish as soon as December 2017.

Given these changes, traditional approaches to cybersecurity in higher education are no longer adequate. While colleges and universities must already deal with a great many government regulations and reporting requirements, NIST 800-171 demands special attention. Institutions that do not comply risk losing federal funding for research and, potentially, financial aid, while those that take a proactive stance stand to gain a competitive advantage. Deadlines for developing a plan of action are rapidly approaching, with the first compliance attestations for defense contracts due at the end of 2017.

To get started down the path to compliance, institutions will first need to understand the challenges that the new standard presents and then chart a course for achieving and sustaining compliance. By drawing on the experiences of institutions further down the NIST 800-171 path, we aim to offer a road map to help institutions comply with the new requirements.

THE LEGAL BASIS FOR PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

In 2010, the White House issued Executive Order 13556, defining CUI. The purpose of the executive order was to gather various information categories—those that required additional protection from disclosure but were not otherwise considered classified information—into a single definition of protected information for all federal agencies. The executive order placed the National Archives and Records Administration in the role of creating a registry of information and handling requirements for the newly defined CUI classification.

As CUI information is often shared among federal agencies and with nonfederal organizations, data handling requirements were needed for the newly defined data type. Charged with creating that guidance, the National Institute of Standards and Technology published Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, in June 2015 (and updated it in January 2016). The requirements outlined in NIST 800-171 apply to CUI that the federal government shares with a nonfederal entity.

The requirement to protect CUI according to a prescribed set of rules is contractual in nature, meaning that nonfederal agencies must scrutinize their contracts with federal agencies and must understand whether any data they receive from a federal agency is classified as CUI. In most instances, federal procurement rules will incorporate the contractual clauses requiring CUI protection. For instance, US defense agencies moved quickly to create a procurement rule that specified that NIST 800-171 is the minimum security standard for protecting any CUI received from defense agencies.

Federal civilian agencies have moved more slowly. While a Federal Acquisition Regulation regarding general data safeguarding came out in 2016 (FAR 52.204-21), the federal government has not yet released a rule mandating that nonfederal agencies protect CUI data received from the government at NIST 800-171 levels. However, a Notice of Proposed Rulemaking was issued in July 2017 stating that a CUI FAR rule would be released in December 2017 and would be open for comment until February 2018, with a final FAR rule to be released shortly thereafter.[4] Until that FAR rule is promulgated, contracts with non-defense federal agencies must specifically reference NIST 800-171 for its requirements to apply to the underlying contract (and associated CUI data).

Traditional approaches to cybersecurity in higher education are no longer adequate. While colleges and universities must already deal with a great many government regulations and reporting requirements, NIST 800-171 demands special attention. Institutions that do not comply risk losing federal funding for research and, potentially, financial aid.

The current state: Where colleges and universities are now

INSTITUTIONS have made varying degrees of progress on NIST 800-171 compliance. While college and university CIOs and CISOs are generally aware of the standard, this awareness hasn't necessarily translated into progress. Many institutions are still working out how to get started and get everyone on board. Other institutions, notably those that receive significant defense research funding, are much further down the path.

In addition, many institutions are not beginning from a common starting point. Institutions that previously built their information security program to a higher standard such as NIST 800-53 have a head start on compliance, whereas 800-171 can represent a much more significant lift for those that haven't built to any standard. For institutions in the latter group, the process ahead will include taking stock of what's already in place, what the new regulations require, and filling in the gaps.

Colleges and universities are also working through how NIST 800-171 will impact their institutional research strategies. Some institutions, for example, view achieving compliance as a potential source of competitive advantage that will help bring in more federal research funding, which, in turn, can help them attract top researchers.[5] Others are stepping back and charting a more conservative path forward, weighing the impact of NIST 800-171 and its associated costs against their institution's desire to build up its research capacity and classification.[6]

To gain traction with institutional leaders, the conversation must be reframed in terms of enterprise risk management, with the business impact to the institution clearly spelled out.

Overcoming the top challenges

Compliance with the spirit of NIST 800-171 goes well beyond technological solutions. To achieve and sustain compliance, it's necessary to take a programmatic approach that encompasses, among other things, organizational change management, training, end user adoption, and process controls. The challenges that institutions face in progressing toward compliance include a lack of executive and board-level attention, significant cultural barriers, and governance coordination.

Lack of executive and board-level attention: While most CIOs and CISOs are aware of NIST 800-171, it is not yet on the radar of many institutional leaders or boards of trustees, largely because the issue has been cast as one of merely implementing a set of technical information security controls. To gain traction with institutional leaders, the conversation must be reframed in terms of enterprise risk management, with the business impact to the institution clearly spelled out. To the extent this is done effectively, resources should follow.

Cultural barriers: Colleges and universities have always enjoyed a culture of openness and sharing. If an American researcher is building on research done by a colleague in another country, it's normal for the two to talk, share information, and even collaborate. Institutional leaders, many of whom rose through the ranks of academia, understand and value this time-honored practice. Outside of defense-related research, the cultural tradition of openness is antithetical to the spirit of protection that NIST 800-171 calls for, and the principal investigator community and others may therefore resist the changes that the standard requires. To pave the way forward, leaders should stress the need for enhanced security while maintaining a federated model for data sharing and access. Institutions should also develop an effective organizational change-management strategy.

Governance coordination: In many institutional settings, responsibility for ensuring contractual compliance lies with the research division. However, as demands grow to comply with International Traffic in Arms Regulations, the Health Insurance Portability and Accountability Act, and other standards, as well as with NIST 800-171, it is no longer effective or economical to do this work in a decentralized manner when there are many research entities that lack the internal capacity to perform compliance. An institutional, enterprise-level solution is needed, as is a central authority to assess and certify data and access compliance.

Getting from here to there: A road map for compliance

INSTITUTIONS approach NIST 800-171 from vastly different circumstances, including the current maturity of their information security programs, the makeup of their research funding portfolio, the structure of their IT programs, and the complexity of their governance processes. As a result, what it takes to achieve compliance will vary widely from institution to institution. That said, there is a common set of activities that all institutions will need to undertake on their path to compliance.

To begin, a college or university should form a working group with representatives from academics, administration, and research; the group should have top-down support and the sustained engagement of leadership. Take Virginia Tech's NIST 800-171 working group, for example: The institution's working group includes senior-level representatives from across the university's IT departments, as well as the university's bursar and registrar, and is jointly sponsored by the university's VP for research and innovation and the VP for information technology.[7]

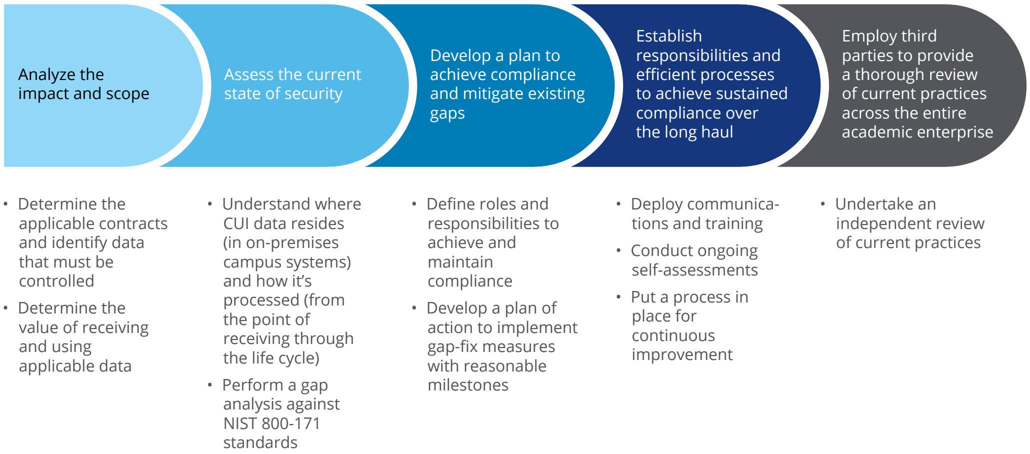
Once formed, the working group should undertake the following five phases of work to manage compliance requirements (see figure 1):

- **Analyze the impact and scope**
  - Determine the applicable contracts and identify data (including student financial data, which may be subject to NIST 800-171 controls in the future) that must be controlled. The level of effort here will be affected by the size and structure of the institution: A smaller institution with a centralized contract/research office will be easier to manage than a large system with decentralized responsibilities over contracting, research, and so forth. Review the contracts to find language related to compliance requirements and references to the data covered. Key questions include the following: What percentage of your institution's current research portfolio is affected by NIST 800-171 requirements? What funding is at stake?
  - Determine the value of receiving and using applicable data: How does it affect critical operations and research? What would happen if the institution were to stop receiving it? This step is important to justify any additional investment. At this stage, some insti-

tutions will need to formulate a preliminary estimate of impact and the cost to comply, and communicate that to senior leadership.

- **Assess the current state of security**
  - Understand where CUI data resides (in on-premise campus systems and in cloud systems) and how it's processed (from the point of receiving through the life cycle): Based on the flow of covered data, understand the security measures already in place to comply with other regulations and standards. This will require getting input from the owners of relevant data and processes, as well as from IT and security representatives. At this point, some institutions may find that they have many controls that meet or exceed NIST 800-171 standards. Others may realize there is significant work ahead and should perform a gap analysis.
  - Perform a gap analysis against NIST 800-171 standards, as needed. Start by interpreting what NIST 800-171 requires and developing a conceptual framework of controls to address standards and compliance. Next, do a crosswalk with any existing standards and regulations that impact the flow of covered data. Once this is done, compliance with any outstanding items in the framework needs to be reviewed. At the conclusion, undertake an updated assessment of impact (specifically on the time, resources, and funds needed to achieve compliance) and communicate the results to senior leadership. As costs become clearer, further decisions on costs and benefits can be undertaken. Some institutions may opt to decline select contracts to avoid undertaking measures to comply.
- **Develop a plan to achieve compliance and mitigate existing gaps**
  - Define roles and responsibilities to achieve and maintain compliance: Based on the assessment's findings, formalize roles and responsibilities to address gaps (using a plan), and maintain any controls going forward.
  - Develop a plan of action to implement gap-fix measures with reasonable milestones.

Figure 1. A road map for NIST 800-171 compliance


Analyze the impact and scope
Assess the current state of security
Develop a plan to achieve compliance and mitigate existing gaps
Establish responsibilities and efficient processes to achieve sustained compliance over the long haul
Employ third parties to provide a thorough review of current practices across the entire academic enterprise
• Determine the applicable contracts and identify data that must be controlled
• Determine the value of receiving and using applicable data
• Understand where CUI data resides (in on-premises campus systems) and how it's processed (from the point of receiving through the life cycle)
• Perform a gap analysis against NIST 800-171 standards
• Define roles and responsibilities to achieve and maintain compliance
• Develop a plan of action to implement gap-fix measures with reasonable milestones
• Deploy communications and training
• Conduct ongoing self-assessments
• Put a process in place for continuous improvement
• Undertake an independent review of current practices

Source: Deloitte analysis.

Deloitte Insights | deloitte.com/insights

It will be important to lock in appropriate financial and leadership support to realistically achieve milestones and to maintain new controls over the long term. The plan must look beyond technical fixes and consider process and governance-related impacts. At this point, institutions should consider funding models needed to achieve and maintain compliance over the long term. Existing security budgets are unlikely to be sufficient to cover these costs. Furthermore, as the institution pursues new federal contracts, each contract should be closely scrutinized and its compliance cost assessed.

- **Establish responsibilities and efficient processes to achieve sustained compliance over the long haul**
  - Deploy communications and training: Based on the institution's plan of action and milestones, identify additional parties affected and engage them in communications and training based on requirements.
  - Conduct ongoing self-assessments: Put a process in place to continually track updates and to assess the ongoing effectiveness of existing controls. Additional gaps may arise based on new contracts and/or changes to the regulations.
  - Put a process in place for continuous improvement: Compliance will be an ongoing process warranting continuous improvement. As new technology arises, consider how it can be applied to more efficiently and effectively address control requirements within the framework of controls an institution has adopted. Existing solutions can help streamline compliance efforts. Many organizations are adopting governance, risk management, and compliance tools that map out regulations and control requirements and can offer dashboards, giving senior leadership visibility into how risks and compliance requirements are being addressed. Because colleges and universities face numerous regulations, it is a good idea to take an enterprisewide approach to compliance with support from technology. This approach is in line with leading practices in commercial enterprises.
- **Employ third parties to provide a thorough review of current practices across the entire academic enterprise**
  - Undertake an independent review of current practices. A third-party evaluation can identify an institution's blind spots; it can also help gain executive and board-level support for addressing any gaps that the review may reveal.

Looking ahead

Up to now, many institutions have struggled to understand how to right-size their institution's security posture, asking, "Are we too strict?" or, "Are we at risk?" While compliance with NIST 800-171 is not without its challenges, the standard sets a common bar for the industry and helps institutions determine whether their security measures are appropriate.

Recommended reading

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. The EDUCAUSE Cybersecurity Program offers a number of resources to help colleges and universities develop and mature their information security and privacy programs. Recommended readings pertaining to the topic of this report include:

- EDUCAUSE, An Introduction to NIST Special Publication 800-171 for Higher Education Institutions (April 2016)
- EDUCAUSE, Information Security Program Assessment Tool (last updated September 2017)
- EDUCAUSE, Digital Capabilities in Higher Education 2016, Information Security Report (forthcoming October 2017)
- Common Solutions Group, NIST SP 800-171 Compliance Template (September 2016)

ENDNOTES

1. Gregory C. Wilshusen, “Federal information security: Actions needed to address challenges,” testimony before the President’s Commission on Enhancing National Cybersecurity, September 19, 2016.
2. Office of Information and Regulatory Affairs, “Federal Acquisition Regulation (FAR); FAR Case 2017-016, Controlled Unclassified Information (CUI),” accessed October 18, 2017.
3. US Department of Education, Office of Student Financial Aid, “Protecting student information,” July 1, 2016.
4. Office of Information and Regulatory Affairs, “Federal Acquisition Regulation.”
5. Deloitte EDUCAUSE working group, July 2017.
6. Ibid.
7. David Brady and T. J. Beckett, “New process and regulations for controlled unclassified information,” Virginia Tech, April 19, 2017.

ABOUT THE AUTHORS

Tiffany Dovey Fishman

Tiffany Dovey Fishman is a senior manager with the Deloitte Center for Higher Education Excellence, responsible for higher education research and thought leadership for Deloitte's higher education practice.

She is on LinkedIn at www.linkedin.com/in/tiffany-fishman-4646133/ and on Twitter @tdoveyfishman.

Richard Rudnicki

Richard Rudnicki is a specialist leader with over 15 years of experience in the Deloitte & Touche Cyber Risk practice, focused on delivering cyber risk and regulatory compliance solutions to clients, with a focus on higher education and the public sector.

He is on LinkedIn at www.linkedin.com/in/richard-rudnicki-1280969/.

Joanna Lyn Grama

Joanna Lyn Grama directs the EDUCAUSE Cybersecurity Initiative and the IT GRC (governance, risk, and compliance) program. She is a member of the US Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

She is on LinkedIn at www.linkedin.com/in/joannagrama and on Twitter @runforserenity.

ACKNOWLEDGEMENTS

In summer 2017, Deloitte and EDUCAUSE convened an expert panel to discuss the implications for higher education institutions in protecting CUI received from the federal government in institutional IT systems. Deloitte and EDUCAUSE extend their thanks to the following working group members: **Ahmed El-Haggen**, CIO and VP for information technology, Coppin State University; **Patrick Feehan**, information security and privacy director, Montgomery College; **Cathy Hubbs**, chief information security officer, American University; **Randy Marchany**, information technology security officer, Virginia Tech; **Ed Martin**, deputy chief information officer, George Washington University; and **Scott Midkiff**, CIO and VP for information technology, Virginia Tech.

Deloitte and EDUCAUSE also wish to extend their thanks to **Timothy D. Sands**, president of Virginia Tech, and **David Swartz**, vice president and CIO of American University, who were interviewed as a part of this project.

This project would not have been possible without the leadership of **Dave Noone**. Thanks also go to **Susan Grajek**, **Cole Clark**, **Allison Eng-Perez**, **Betty Fleurimond**, **Justin Williams**, **Michael Wyatt**, **Srini Subramanian**, and **Devin Amato**.

CONTACTS

Betty Fleurimond
Managing director, higher education
Deloitte Services LP
+1 202 492 1453
bfleurimond@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

Joanna Lyn Grama
Director of cybersecurity and IT GRC programs
EDUCAUSE
+1 720 406 6769
jgrama@educause.edu

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Contributors
Editorial: Matthew Budman, Nikita Garia, Abrar Khan
Creative: Kevin Weier
Promotion: Haley Pearson
Artwork: Alex Nabaum

About Deloitte Insights
Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication
This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

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. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.