EDUCAUSE

**Response to NIST RFI: "Developing a Framework to Improve Critical Infrastructure Cybersecurity"**

Submitted by: EDUCAUSE and Internet2 Higher Education Information Security Council (HEISC)
Primary Contact: Rodney Petersen, Managing Director, Washington Office, EDUCAUSE

## Introduction

The Higher Education Information Security Council (HEISC), hosted by EDUCAUSE and Internet2, is pleased to submit comments to the Request For Information on Developing a Framework to Improve Critical Infrastructure Cybersecurity. Although colleges and universities are not identified as a critical infrastructure in current government policy, we are owners and operators of some of the largest and most powerful computer systems in the world and our interdependencies with both the government and private sector make institutions of higher education an important player in the overall cyber ecosystem.

## Background About the Higher Education Sector

The higher education sector is comprised of an extremely diverse set of institutions that makes the application of "standards" and "practices" difficult to achieve without a significant degree of flexibility and nuance. There are over 4,500 colleges and universities in the United States. Although seventy percent of those institutions are private or independent – and typically small- to mid-size – and 30 percent are public institutions that receive some level of state financial assistance and oversight, over 70 percent of students are educated at public colleges and universities that include two-year or community colleges. While a large university may be similar in many respects to a large enterprise in the private sector, the most institutions of higher education are small and are the equivalent of a small business. Additionally, the not-for-profit sector of higher education is dependent on tuition, fees, private donors, and public assistance to support the educational and research mission.

The culture of higher education is one that highly values autonomy, freedom, collaboration and sharing, decentralized administration, and distributed decision-making (i.e., faculty governance). These cultural factors combined with limited resources make it a challenge to institute cybersecurity practices in higher education. Nonetheless, the academic setting has been the source of some of the greatest innovations in networked information technologies and are the testbed for many of the current challenges confronting corporate America. For example, as the federal government and companies struggle to address the challenges of Bring Your Own Device (BYOD) students, faculty, and guests have been bringing personally-owned computers and accessing the campus network for years.

## Information Security Guide for Higher Education

The National Strategy to Secure Cyberspace issued in February 2003 proposed the following action:

> Colleges and universities are encouraged to secure their cyber systems by establishing some or all of the following as appropriate: (1) one or more ISACs to deal with cyber attacks and vulnerabilities; (2) model guidelines empowering Chief Information Officers (CIOs) to address cybersecurity; (3) one or more sets of best practices for IT security; and, (4) model user awareness programs and materials.

Accordingly, the Higher Education Information Security Council (HEISC) immediately moved to establish the "Information Security Guide: Effective Practices and Solutions for Higher Education" (http://www.educause.edu/security/guide) that is the premier source for standards, practices, and resources for the higher education community.  Organized according to the ISO 27002 Code of Practice for Information Security Management, the Guide also cross-references other standards such as those developed by NIST, COBIT (A Business and Governance Framework for the Management of Enterprise IT), and the Payment Card Industry Data Security Standard (PCIDSS).  The Guide consists of an overview of the standard and practice objectives, examples of effective practices and solutions contributed by the higher education community, and links to other resources that come from higher education, government, and industry.  Although the Guide and the ISO standard has served HEISC and the higher education community well for the past decade and beyond, we are also eager to sync up with any emerging standards or practices which is why we are closely following NIST's activities in response to the President's recently issued Executive Order on Improving Critical Infrastructure Cybersecurity.

We have convened a couple of open meetings of the higher education community over the past few weeks to develop responses to as many of the questions as possible contained in the Request for Information.  Below is a summary of our responses.

## Current Risk Management Practices

**1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?**

Implementation of a new framework for colleges and universities will prove challenging due to departmental budgets, varying expertise of existing security staff (or lack of full-time security staff), and availability of reasonably priced tools. Educating executive and middle management on the threats, risks, and cost may also delay improvement of cybersecurity practices.

Other challenges include: insider threats, obsolete campus equipment, poor access control, outdated authentication standards, simple protocols, and embedded devices that require additional patching or do not have the ability to run antivirus software or encryption protocols.

**2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?**

Colleges and universities must comply with various legislative requirements at the federal, state, and local level while public institutions are also dealing with different public records requirements. Institutions also have many highly proprietary systems or software. And since institutions vary in size, financial resources, and staff, they often need to focus on different risks or priorities.

There is a willingness to collaborate and compromise across sectors and develop a common body of knowledge, but there will be domain-specific technical knowledge that does not necessarily span all sectors. It may be necessary to develop a cybersecurity framework for each critical infrastructure that is unique to that sector, but baseline security standards may go a long way towards making progress in terms of risk.

**3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?**

Institutions of higher education typically have a governance body that includes key senior management stakeholders and oversees the process for developing risk-related policies and procedures. The most difficult part of establishing a risk policy at an institution is identifying who has authority to accept the risk. Policies and procedures may be communicated on the website or through e-mail to staff and faculty.

**4. Where do organizations locate their cybersecurity risk management program/office?**

At colleges and universities, Information Security programs/offices are typically located within the central Information Technology (IT) department, although they may be located within the Office of the Risk Officer, the President's Office, or the Office of Public Safety. The Chief Information Security Officer (CISO) usually reports to the Chief Information Officer (CIO) or Vice President for IT.

**5. How do organizations define and assess risk generally and cybersecurity risk specifically?**

Although the initial focus may have been on cybersecurity risks, many colleges and universities are currently developing a formal IT risk management or Enterprise Risk Management program to promote data protection across the institution. Many of these risk programs are based on ISO or NIST standards, as well as the SANS 20 Critical Security Controls, and include campus-wide business and academic processes, information, and asset owners. Risk assessments are not restricted to technical controls or electronic information, but also address paper documents and manual business processes where applicable.

Risks to the higher education community include hacktivists (i.e., anonymous group attacks on multiple universities in 2012) and cyber-criminal groups harvesting data and causing compromised identities of students, faculty, staff, alumni, and local community members. Colleges and universities are particularly vulnerable to attacks because of the long-standing culture of academic freedom, openness, and sharing.

**6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?**

Cybersecurity risk is often incorporated into an institution's enterprise risk management (ERM) program. ERM is becoming a high priority for campuses, especially as enterprise applications and services are being outsourced to cloud vendors or solution providers. In addition to monitoring an institution's own risks and threats, they are now required to deal with third party vendors that may host sensitive data. Although much institutional attention has been devoted towards protecting human assets (especially as a result of active-shooter tragedies) or physical assets (especially in response to natural disasters such as hurricanes), cyber assets are increasingly deemed as mission-critical since so many institutional processes and services rely on network availability and online services.

**7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?**

Colleges and universities are being encouraged to implement the InCommon Assurance Program, which awards certifications to qualifying campuses and non-profit sponsored partners and research organizations that comply with the InCommon requirements for consistent electronic credential and identity management practices. These practices determine the confidence in the accuracy of a user's electronic identity and help mitigate risks. The InCommon Community developed these profiles for research and education to satisfy the Federal Identity Credential and Access Management requirements which references NIST 800-63 as the basis for their program. The Bronze and Silver Profiles were written for and by Higher Education implementers and are comparable to levels 1 and 2 outlined by NIST. InCommon's profiles reference password techniques only, but allow approved alternative means to be used.

Institutions also use the SANS 20 Critical Controls as procedural guidance for an information security program.

Operational security issues are shared among the higher education community through the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC). Best practices are collected in the Information Security Guide for higher education.

Other standards, guidelines, best practices, or tools used by the higher education community for enterprise cybersecurity include:

- NIST 800 series
- ISO 27000 series
- COBIT framework
- Information Technology Infrastructure Library (ITIL)
- Information Technology (IT) Governance, Risk, and Compliance (GRC) or Enterprise GRC applications with risk, threat, and policy management modules - e.g., Modulo or Brinqa
- COSO Internal Control - Integrated Framework
- Payment Card Industry Data Security Standards (PCI DSS)
- HITRUST Common Security Framework (CSF)
- ISACA Risk IT Framework
- Texas Administrative Code, Chapter 202 (TAC 202): Information Security Standards
- Factor Analysis of Information Risk (FAIR) framework
- North Dakota Statewide Information Technology Plan (2013-2015)

It's important to note that any set of standards should not be considered "bullet-proof" and could be viewed as a blueprint as to what to attack. Standards also tend to lag behind "state of the art" cybersecurity tools, technologies, and risks.

**8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?**

National regulatory and compliance requirements relating to cybersecurity for the higher education sector include: FERPA, HIPAA, GLBA, COPPA, export controls (ITAR and EAR), ECPA, and FISMA. For a complete listing of higher education compliance issues and resources, see the Higher Education Compliance Alliance.

State regulatory and compliance requirements include individual state data breach notification and reporting laws for personally identifiable information (PII) and public records requests. State security standards may be a factor for some institutions, as well (e.g., Virginia, Texas, and Maryland).

**9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?**

Public safety is a critical function on every campus. Cyber attacks may affect first responders and emergency response at the campus, local, and state levels, as well as medical hospitals during a major emergency.

More generally, colleges and universities have interdependencies on external infrastructures such as financial services, energy, water, telecommunications, healthcare, food industries, internet providers, and transportation. Campuses are like small cities and control certain areas, but rely on local, regional, and national infrastructures in order to operate. (Note that many universities are responsible for running and maintaining regional or state networks, as well as K-12 school networks and data centers.)

Research centers or facilities, especially those housing experimental animals, are also considered a critical asset by universities (see Tulane's experience during Katrina).

**10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?**

Institutions of higher education try to attain a balance between satisfying institutional business and academic goals and objectives while providing a robust, effective, safe and reliable information technology and cyber security infrastructure.

**11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?**

Some institutions are required to submit a strategic technology plan to the state.

**12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?**

Some institutions provide guidance and benchmarking tools, while others offer "umbrella" frameworks that consider the roles of people, process, and technology, that can be used to take a comprehensive approach.

## Use of Frameworks, Standards, Guidelines, and Best Practices

**1. What additional approaches already exist?**

Existing approaches commonly used by colleges and universities include the ISO 27000 series and the NIST 800 series.  Colleges and universities are also expected to comply with contractual obligations under the Payment Card Industry Data Security Standard (PCI DSS)

**2. Which of these approaches apply across sectors?**

The ISO 27000 series and the NIST 800 series could be applied across sectors. Although there are mappings and "crosswalks" for various standards, incorporating ISO and NIST into one standard would prove beneficial to all sectors.

**3. Which organizations use these approaches?**

HEISC encourages colleges and universities to use the ISO 27000 standard. Institutions such as Georgia State University, the University of Tampa, the University of Texas System, and Indiana University use the ISO standard. The University of Florida and the University of Tampa also use the NIST 800 series.

**4. What, if any, are the limitations of using such approaches?**

There are a number of competing standards, and selecting a single standard will be difficult. Existing requirements (e.g., HIPAA or FISMA) can be too broad, so a more prescriptive framework or standard with a focus on prevention (e.g., PCI DSS or the SANS 20 Critical Security Controls) would be helpful. A limitation of more prescriptive requirements with rapidly changing technologies would be the need to provide updates more frequently.

Some of the ISO standards from the 27000 series were last revised in 2005 and do not address the current threat landscape and thus supplemental resources are necessary.

The existing controls in the NIST 800 series target government systems and methods; other sectors such as higher education are not incorporated. Current requirements are too broad or comprehensive and few allow for maturation of the information security program. NIST guidance could be better if an umbrella approach is taken to tell organizations *what to do*, provide general guidance on *how to do it*, and show additional guidance on *measuring effectiveness*. NIST could also benefit from incorporating the ISO approach and assist organizations who are early in the maturity cycle of their information security programs.

**5. What, if any, modifications could make these approaches more useful?**

Addressing cybersecurity issues associated with critical infrastructure requires focused attention supported by resources: people, facilities, information, and funding. Imposing unfunded mandates at the federal level would prove challenging for higher education, especially if specific configurations would be required from a top-down perspective. Additionally, many colleges and universities hire consultants to implement NIST standards or assess the institution against NIST standards and these additional expenses could be rerouted to fund information security programs.

Approaches could be more useful by:

- Providing recommendations to secure top-level buy-in;
- Emphasizing asset inventory and categorization;
- Providing guidance that is easy to understand and incorporate;
- Offering an approach that produces early wins for new programs and is not only geared towards well-funded or well-staffed organizations;
- Simplifying the approach to risk management and the controls in NIST 800-53;
- Incorporating maturation into the assessment process;
- Identifying and prioritizing top controls;
- Providing training and awareness at a reasonable cost that is geared towards faculty, staff, and new hires, as well as those in financial and healthcare sectors;

**6. How do these approaches take into account sector-specific needs?**

Higher education has many unique challenges and opportunities that existing approaches used by other industries do not take into account. Consider the following needs:

- Balance security with academic freedom (e.g., how to secure the infrastructure while allowing computer science students to reverse engineer malware or hack into specific systems).
- Look beyond US-centric approaches since many organizations are global.
- Take decentralized approaches to security into account.
- Address organizations that have “transitory” populations (e.g., students, visitors).
- Address the need to collaborate and share data or work material with others in the same organization or other organizations.
- Provide guidance on open source or free tools.
- Provide a coherent set of compliance and regulatory requirements.

The categorization of organizations as "sectors" is also difficult because some institutions of higher education operate more like a municipality than an enterprise. Many will develop and maintain their own roads, electricity, sewer, telecommunications, and other infrastructure. They may also employ their own police and fire departments for emergency services. Institutions of higher education have very diverse approaches and needs in terms of infrastructure and services when compared to an enterprise that outsources most of this to someone else where it is their responsibility.

**7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?**

We use the term "effective practices and solutions" rather than "best practice" within our sector because of the recognition that "one size does not fit all". For example, what works for a large research university may not scale well for a small liberal arts college. Therefore, it would be nice if the "framework" could be general enough that more sector-specific standards or practices could be developed and adopted that are effective – and realistic. That is not to say that there is no benefit in cross-sector collaboration or sharing of standards and practices. Whatever process that ensues should be flexible enough to take into account the diversity of types of organizations, relative approaches to risk, and the degree to which resources can be effectively applied.

**8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?**

The Higher Education Information Security Council (HEISC), as the sector coordinating council for colleges and universities, has an existing team that serves as editors for our Information Security Guide. HEISC and its volunteers stand ready to monitor the NIST framework, participate in the process as much as possible, and incorporate any future guidance or resources into our current approach.

Standards should be easily accessible (as NIST is now) and provide materials that sectors can use in their organizations to gain support for them with business and academic leadership. (i.e., Reader's Digest formats as opposed to the much larger standards publications).

Within the standards documents, or as a separate companion piece, mappings and integration guidance should be provided with other popular standards, requirements, or guidelines (e.g., ISO 27000 series, ITIL, PCI DSS, HIPAA, GLBA, COBIT, etc.) to assist organizations in their compliance efforts.

**9. What other outreach efforts would be helpful?**

It would be useful to provide low-cost or no-cost training to groups from every sector, similar to what US-CERT does, by offering free training courses and materials to help security practitioners. Training should be promoted and provided across the country or through web-based offerings.

Each sector should be involved in the development of standards.

## Specific Industry Practices (12 questions)

**1. Are these practices widely used throughout critical infrastructure and industry?**

Most of these practices are widely used in higher education since they are incorporated within the ISO 27000 standards. Some practices may be employed to a different extent than private industry (e.g., privacy and civil liberties protection may be a higher priority for colleges and universities).

Institutions may target areas or departments that are more at risk whereas the private sector may apply the same controls across the entire organization.

**2. How do these practices relate to existing international standards and practices?**

While ISO and NIST standards have served as frameworks for many colleges and universities in the past, several of the reviewers of the RFI commented that the proposed categories are far more useful than the existing labels for the chapters of ISO or the sections of NIST standards.

**3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?**

For colleges and universities, it varies according to threat probability, threat impact, and appetite for risk. However the most critical practices for the secure operation of critical infrastructure would be:

- Identification and authorization of users accessing systems;
- Separation of business from operational systems (e.g., network segmentation on campuses);
- Asset identification and management (i.e., establishing controls can help an organization understand where information lives and better protect the data);
- Monitoring and incident detection tools and capabilities (i.e., being more proactive than reactive);
- Use of encryption and key management (i.e., better protecting sensitive data due to provisions of state breach laws);
- Security engineering practices (including secure application development);
- Mission/system resiliency practices.

**4. Are some of these practices not applicable for business or mission needs within particular sectors?**

We believe that each of these categories would apply to colleges or universities, although the methods for achieving them may vary across institutions.

**5. Which of these practices pose the most significant implementation challenge?**

Asset identification and management: Asset identification is difficult because many campuses are decentralized. Prioritization is also difficult because of competing school or departmental missions. Additionally, institutions have many ways to purchase something and it is difficult to know what we have and who owns it (e.g., items could be purchased through grant funds or items are below the threshold of notification). Regarding grant-funded purchases, researchers often need specialized equipment that does not readily allow for compliance with institutional standards. Another asset identification challenge is portable devices, whether it is a personally owned device or provided by the institution.

Use of encryption and key management: There are a number of ways to implement encryption. Institutions do not follow one standard or best practice for encrypting devices.

Although data classification and data loss prevention are not listed as one of the suggested practices, colleges and universities are very concerned with these issues. At this time, it is difficult to implement data classification at an institution, especially for research data.

Regarding identification and authorization of users accessing systems, institutions are required to provide different types of access for staff, faculty, and students who may have multiple roles on a campus.

**6. How are standards or guidelines utilized by organizations in the implementation of these practices?**

The ISO 27000 standards offer guidance on *what to do*, not *how to do it*, so implementation of controls is still a big challenge for institutions. Colleges and universities may rely heavily on third parties, which means increased costs or budgetary challenges and less money for institutional staffing or program funding.

**7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?**

Colleges and universities rarely have enough resource for standards development internally so they turn to national organizations such as EDUCAUSE or HEISC to document a community of practice.  There has been insufficient investment to date – at both the campus level and association level – to the process of standards development.  Thus, we tend to rely heavily on resources developed by others including NIST and other standards bodies.

**8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?**

This varies largely from campus to campus.  The advent of data exposure incidents have forced most colleges and universities to organize incident response teams to both respond to incidents and work proactively to prevent them.  The Research and Education Networking ISAC (REN-ISAC) also provides early threat notifications to institutions that can help them prevent attacks.  The ownership for cybersecurity largely rests with the CIO or CISO at a college or university so that formalization of policies and processes usually depends on the maturity of the information program and the level of investment.

**9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?**

Mobile devices (especially personally owned devices on campus) pose a risk to any organization. Some sectors may be able to require encryption of all mobile devices and remotely wipe any lost devices. Institutions run into challenges if the mobile device is used for work and personal purposes - i.e., can personal data be wiped to protect the university.

Key management, cited above, usually implies key escrow, which in turn implies a loss of privacy versus encryption.

Monitoring network traffic and network access that could lead to the identification of individuals and their actions would be a concern among institutions.

Data loss prevention could be seen as an invasion of privacy if institutions are searching a professor’s e-mail to determine where data may be leaking.

**10. What are the international implications of this framework on your global business or in policymaking in other countries?**

Many colleges and universities have campuses located in other countries and/or have faculty, staff, and students traveling abroad. Guidance should be provided on export controls, encryption of mobile devices, and international privacy laws. However, international laws are so widely varied that establishing a framework that can be applied in all countries will be challenging.

**11. How should any risks to privacy and civil liberties be managed?**

There is a need to balance security measures and privacy, especially in academic spaces. It is important to develop a framework for addressing privacy concerns as security postures are enhanced with more robust technologies. (California institutions are currently developing a privacy framework that will address information privacy (i.e., data) and autonomy privacy (i.e., rights of individuals).)

Clear guidelines and policies, including appropriate approvals, should be established to control access to information that individuals may consider “private” such as e-mail. Involving key stakeholders in the process and having them take ownership of compliance efforts in their areas is important.

Training and awareness is also necessary to make people aware of the data they handle, which data they can access, and the related policies of the institutions.

**12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?**

The standards that apply to cybersecurity may not necessarily be the same as practices for information security (that includes the protection of information in print or non-digital form). Increasingly, we are trying to move colleges and universities away from a cyber and IT-only orientation to an information protection point of view that seeks to be comprehensive in its approach to the security of data and information. Consequently, the extent to which the framework can incorporate the domains of people, process, and technology will be useful as a future-oriented approach to information and infrastructure security.