SESSION #BO15

Institutions of Higher Education and Controlled Unclassified Information

Mia Jordan

U.S. Department of Education

2020 Virtual FSA Training Conference for Financial Aid Professionals

Federal Student Aid

An OFFICE of the U.S. DEPARTMENT of EDUCATION

AGENDA

01 Overview

02 Driving the Change

03 NIST SP 800-171

04 Future State

OVERVIEW

WHY ARE WE HERE?

- Cybersecurity incidents\risk - increasing on Institution Campuses
- Technology use is rapidly evolving while the ability to protect the information is falling behind
- IHEs handle some of the most sensitive financial and privacy data
- The Federal government has mandated additional protective measures for data that is deemed to be sensitive and classified as Controlled Unclassified Information (CUI). Examples of CUI:
  - Privacy Information: Military Personnel Records, Personnel Records, Student Records, Sensitive Personally Identifiable Information
  - Federal Taxpayer Information
  - Financial: Electronic Funds Transfer, Financial Supervision Information, General Financial Information
- Applies to Federal contractors, subcontractors, state, local, and tribal governments, colleges and universities

CAMPUS CYBERSECURITY PROGRAM

Mission

Monitor and reduce cybersecurity risks to enhance the protection of FSA student financial assistance program data, which are collected, received, processed, stored, transmitted, or destroyed by FSA, IHEs, and third-party servicers.

Vision

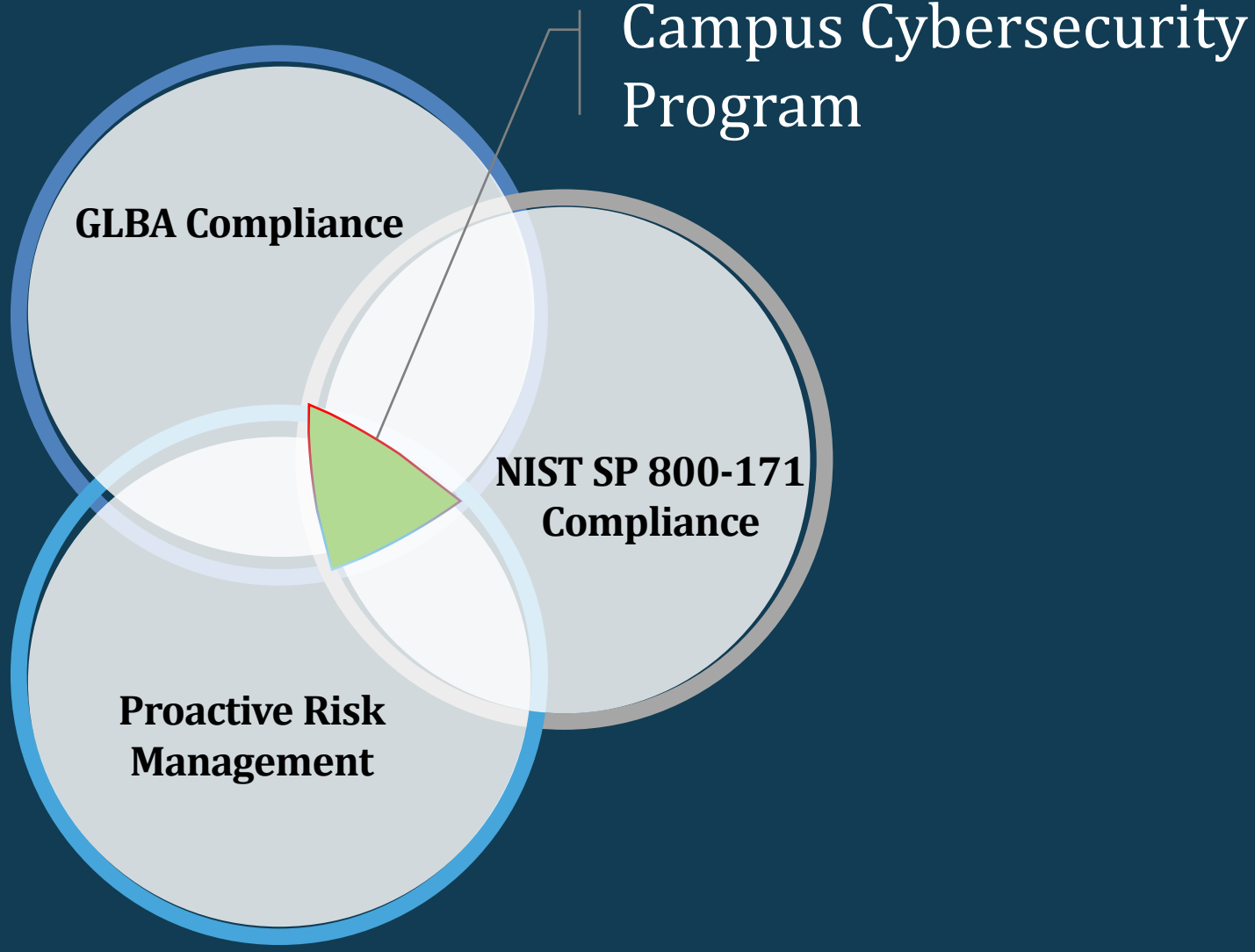
Enable America's students and borrowers to confidently participate in federal financial assistance education programs knowing that their financial information and the integrity of their transactions are protected.

Objectives

- Educate, support, and incentivize partners to mature their cybersecurity postures;
- Address the mandate to protect CUI;
- Oversee and support IHE compliance with the Gramm-Leach-Bliley Act (GLBA) as well as other applicable mandates; and
- Mature FSA's Title IV data breach capabilities and processes.

DRIVING THE CHANGE

OUR FOCUS


Campus Cybersecurity Program
GLBA Compliance
NIST SP 800-171 Compliance
Proactive Risk Management

PROGRAM GOALS

Understand Risks

Provide visibility into Institutions of Higher Education (IHE) compliance with Federal guidelines and their maturity level

Identify Trends

Identify trends that differentiate IHEs with more mature cybersecurity security postures vs IHEs that need some support to enhance their program

Aid Decisions

Provide a holistic view of the cybersecurity posture of IHEs to facilitate program decisions

NIST SP 800-171

THE DRIVER

Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

-- Executive Order 13556

WHY A STANDARD FRAMEWORK?

- Over 100 different ways of characterizing sensitive information
- No common definition or protocols
- Information inconsistently marked
- Common definition and standardize processes and procedures
- CUI Protection requirements are defined in National Institute of Standards and Technology (NIST) Special Publication NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

WHAT IS NIST 800-171?

NIST Special Publication 800-171 defines the security requirements (controls) required to protect CUI in nonfederal information systems and organizations.

- Information systems that process, store, or transmit CUI may be federal or nonfederal
- When federal (including contractors operating on behalf of), agency security requirements are applied
- When non-federal, SP 800-171 security requirements are applied

NIST 800-171 – THE SIMPLE VERSION

1. Access Control: Who is authorized to view this data?
2. Awareness and Training: Are people properly instructed in how to treat this info?
3. Audit and Accountability: Are records kept of authorized and unauthorized access? Can violators be identified?
4. Configuration Management: How are your networks and safety protocols built and documented?
5. Identification and Authentication: What users are approved to access CUI and how are they verified prior to granting them access?
6. Incident Response: What's the process if a breach or security threat occurs, including proper notification?
7. Maintenance: What timeline exists for routine maintenance, and who is responsible?

The 14 Points of NIST 800-171 - https://www.kelsercorp.com/blog/everything-you-need-to-know-about-nist-800-171

NIST 800-171 – THE SIMPLE VERSION

8. Media Protection: How are electronic and hard copy records and backups safely stored? Who has access?
9. Physical Protection: Who has access to systems, equipment and storage environments?
10. Personnel Security: How are employees screened prior to granting them access to CUI?
11. Risk Assessment: Are defenses tested in simulations? Are operations or individuals verified regularly?
12. Security Assessment: Are processes and procedures still effective? Are improvements needed?
13. System and Communications Protection: Is information regularly monitored and controlled at key internal and external transmission points?
14. System and Information Integrity: How quickly are possible threats detected, identified and corrected?

The 14 Points of NIST 800-171 - https://www.kelsercorp.com/blog/everything-you-need-to-know-about-nist-800-171

FUTURE STATE

GENERAL PLANNING ASSUMPTIONS

IHEs have information technology infrastructures in place.

- They are not developing or acquiring systems specifically for the purpose of processing, storing, or transmitting CUI

IHEs have safeguarding measures in place to protect their information.

- May also be sufficient to satisfy the CUI requirements

IHEs may not have the necessary organizational structure or resources to satisfy every CUI security requirement.

- Can implement alternative, but equally effective, security measures
- Can implement a variety of potential security solutions
- Directly or by using managed services

PREREQUISITES

The Campus Cybersecurity program is approved by Department leadership:

- FSA is resourced and prepared to implement the program
- Multi-year timelines are appropriate to requested actions
- Training and outreach sessions are available

FSA has a formal CUI program in place.

- Information and data are properly marked and tagged

TIMING

Near-Term

- Electronic Announcement – mid Dec 2020
- Engage community stakeholders
- IHE self-assessment
- Educate IHEs

Intermediate-Term

- Collect IHE cybersecurity data
- Implement IHE risk profiles
- Initiate pilot using risk profiles

Long-Term

- Fulfill ED and FSA CUI mandate
- Refine IHE support structure

IHE NEXT STEPS…

1. Review the Electronic Announcement – planned for release mid Dec 2020.
2. Conduct a self-assessment – guidance will be provided by FSA
   - Some security controls may not be applicable to your environment
   - Build off what you are currently doing
   - There may be other ways to meet the requirements
3. Look at some cost-effective best practices:
   - Isolate CUI into its own security domain by applying architectural design concepts
   - Security domains may employ physical separation, logical separation, or a combination of both
   - Use the same CUI infrastructure for multiple government contracts or agreements

QUESTIONS

Mia Jordan

Email: FSA_IHECyberCompliance@ed.gov