OWENS
COMMUNITY COLLEGE

Gramm-Leach-Bliley Act (GLBA)

Data Security Program

Table of Contents

Overview

Institutions who participate in the Federal Student Aid programs under Title IV of the Higher Education Act of 1965, as amended, are considered to be “financial institutions” per the Gramm-Leach-Bliley Act (GLBA 2002), as implemented in regulation under Title 16, Part 314 of the Code of Federal Regulations.

Due to this designation, Owens Community College is required to have safeguards in place in order to protect the confidentiality, integrity, and availability of protected data.

The GLBA Safeguards are defined at a high-level as the following:

- Develop, implement, and maintain a written comprehensive information security program

- Designate an employee or employees to coordinate the program

- Identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments of:
    - Employee training and management
    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal
    - Detecting, preventing and responding to attacks, intrusions, or other systems failures

- Control the risks identified, by designing and implementing information safeguards and regularly test or monitor their effectiveness

- Oversee service providers, by:
    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for Federal Student Aid, student, and school (customer) information at issue
    - Requiring your service providers by contract to implement and maintain such safeguards

- Evaluate and adjust the information security program based on the results of testing and monitoring, changes to operations or business practices, or other circumstances with a material impact on the information security program

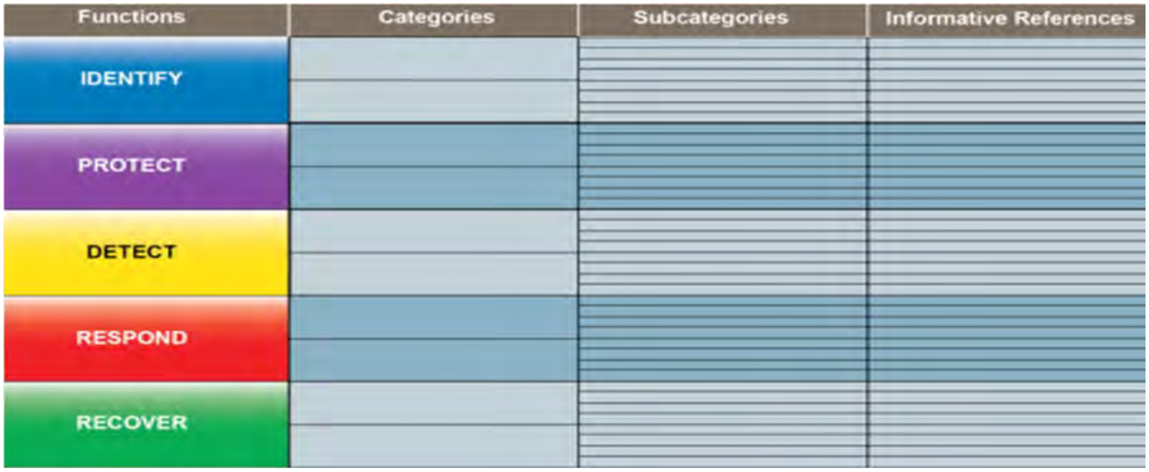
These requirements are also referenced in the U.S. Department of Education’s Dear Colleague Letter GEN-16-12 published on July 1, 2016 (Appendix C), and are subject to audit under the Single Audit Act (often referred to as an A-133 Audit).

GLBA Safeguards

Develop, implement, and maintain a written comprehensive information security program

Information Technology Services (ITS) at Owens is responsible for containing administrative, technical, and physical safeguards that are appropriate for the size, complexity, and nature of its activities, in order to: (1) Ensure the security and confidentiality of customer records and information; (2) Protect against any anticipated threats or hazards to the security or integrity of such records; (3) Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

The Chief Information Officer (CIO) at Owens is responsible for maintaining the documentation of the College's Information Security Management System (ISMS), which includes many elements of the GLBA Compliance Program. This program follows the NIST Framework which is depicted in the following chart.



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Designate an employee or employees to coordinate the program

All affected functional offices at Owens are responsible for day-to-day compliance. The following individuals are responsible for oversight and coordination of the program.

Department	Designee
Information Technology Services (ITS)	Brian Lauber, Chief Information Officer
Office of Financial Aid	Andrea Morrow, Director
Office of Student Accounts	Todd Schroeder, Director

Identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments

The Chief Information Officer maintains documentation regarding the Security Risk Assessments performed by the College.

The risk assessment includes a review of the following components.

Employee training and management

One of the most serious threats to the confidentiality, integrity, and availability of nonpublic personal information is through errors made on the part of employees. Often this is due to the employee not being familiar with proper procedures for handling such information. Owens Community College uses KnowBe4 online training modules to train employees. All new employees are automatically assigned training as part of their onboarding as well as required employees will receive online annual training. Owens Community College also occasionally performs “phishing campaigns” to help train employees on how to spot a phishing attack.

Information systems, including network and software design, as well as information processing, storage, transmission, and disposal

Owens Community College stores nonpublic personal information in both paper form and electronically. Preventing unauthorized access to both of these types of records is a crucial part of Owens Community College’s Information Security Program.

Paper records with nonpublic personal information are stored in locations that have restricted access. Each department is responsible for making sure their records are stored in a secure location. Electronic Records are stored on servers and protected with limited access. The physical servers are stored in a location with limited access. Access of nonpublic personal information in the College’s Enterprise Resource Planning system is encrypted in transit. Documents with nonpublic personal information that aren’t disposed of correctly also pose a risk. Owens uses Allshred to securely dispose of documents with nonpublic personal information.

Owens also recognizes that security risks continue to evolve and there is a need to have security assessments performed. In FY20, Owens had a security maturity assessment performed and continue to perform on going risk assessments through vulnerability scans and penetration tests.

Detecting, preventing and responding to attacks, intrusions, or other systems failures

Owens recognizes that the risks associated with these are always evolving and we continually evaluate our information security program. Owens uses syslog servers, monitoring software, and security information and event management software to identify potential attacks, intrusions or other system failures.

Control the risks identified, by designing and implementing information safeguards and regularly test or monitor their effectiveness

Owens utilizes the following controls and safeguards, which have been identified using the results from the risk assessment and based on best practices. The information below is organized in accordance with the requirements outlined in NIST (National Institute of Standards and Technology) SP (Special Publication) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations". This standard requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Federal policies. NIST SP 800-171 identifies specific recommended requirements for non-Federal entities that handle Controlled Unclassified Information (CUI). Please see the Owens Information Security Management System document for more details regarding these processes. *Numbers in parentheses refer to the corresponding section of the NIST standard.*

- **Access Control Requirements (3.1): Limit information system access to authorized users**
  - Access to systems (shared network resources, Banner, OnBase, etc.) is requested through the Access store. The supervisor and the data manager of the content area must approve the access before it is granted. Access Store is only available on campus
  - Using Banner SIS security roles, we limit system access to the types of transactions and functions that authorized users are permitted to execute
  - We separate non-privileged, privileged and administrator accounts in our information systems
  - Banner SIS audit logs track the execution of privileged functions
  - Critical systems limit unsuccessful login attempts
  - Screen saver / monitor lock on computers
  - Inactive user sessions are terminated after the time-out period
  - Remote access to critical systems is only allowed through secured, encrypted VPN
  - Administrative wireless access is encrypted and requires prior authorization and authentication once granted

- **Awareness and Training Requirements (3.2): Ensure that system users are properly trained**
  - ITS is available upon request to provide updates, presentations and training to all GLBA impacted staff
  - Upon being approved for access to financial aid data in the college's information systems, a user receives the "Access and Use of Financial Aid Data" guidelines from the Office of Financial Aid
  - Appropriate use of confidential information is included in the following Board of Trustees policies and procedures:
    - Standards of Conduct (3358:11-5-52)
    - Information Technology Policy (3358:11-6-01)
    - Data Use and Protection Policy (3358:11-6-02)
  - Training regarding use of specific modules is the responsibility of the departments
  - ITS offers online training modules to faculty and staff for security awareness

- **Audit and Accountability Requirements (3.3): Create information system audit records**
  - Audit logs with username associations are stored in Banner tables and in OnBase
  - Splunk as a Security Information and Event Management system
  - NTP is used to ensure all system clocks synchronize
  - Access to audit logs is limited to authorized users

- **Configuration Management Requirements (3.4): Establish baseline configurations and inventories of systems**
  - Inventory of Systems is documented
  - Configuration of desktops is managed by ITS Client Services
  - Banner has baseline configuration for new user creation and inventory of modules
  - Changes on organizational systems either go through change control or IT Governance
  - Principle of least privilege is followed when granting access to systems
  - AppLocker is used to prevent unauthorized applications from launching
  - Users can only install ITS approved and tested software
  - Annual access review for Banner

- **Identification and Authentication Requirements (3.5): Identify and authenticate users appropriately**
  - Password complexity
    - At least six characters long
    - Include at least one number
    - Can't reuse a previous password
  - Password expires every 120 days
  - Usernames are not re-used
  - 6 failed attempts to Banner locks account

- **Incident Response Requirements (3.6): Establish incident-handling capability**
  - ITS uses several tools to monitor the network and systems for attacks and anomalies.
  - Owens has an IT Incident Response (**Appendix A**) plan in the event of a known or suspected breach.

- **Maintenance Requirements (3.7): Perform appropriate maintenance on information systems**
  - Banner/Onbase routine maintenance
  - SCCM patches to desktop
  - Requirement to DoD 5220.22-M wipe before being recycled
  - Endpoint security through Microsoft Security Center and AppBlocker

- **Media Protection Requirements (3.8): Protect media, both paper and digital, containing sensitive information**
  - Office of Financial Aid has procedures for physical protection of paper media
    - Policy on shredding and recycling
  - Requirement to DoD 5220.22-M wipe drives before being repurposed or recycled
  - Offsite backups are encrypted

- **Personnel Security Requirements (3.9): Screen individuals prior to authorizing access (;**
  - Human Resources background check
  - Job postings for positions in the Office of Financial Aid require an individual to meet requirements for Federal Student Aid system access.
  - Procedure in place to remove access when terminations occur
  - All employees sign a confidentiality agreement

- **Physical Protection Requirements (3.10): Limit physical access to systems**
  - Central servers containing data are in data center with restricted access
  - Audit logs are maintained of access to the data center for both employees and guests
    - Limit access to Student Accounts Scan and File room by locking room when not in use
    - The Office of Financial Aid staff offices are locked when the employee is not on site Shared printing and scanning resources are located in offices which are surrounded by staff offices to allow for monitoring of those locations. When the office is closed, those locations are locked
    - The Mail Center mailboxes require a combination code for access.

- **Risk Assessment Requirements (3.11): Conduct risk assessments**
  - Vulnerability scans periodically
  - A risk assessment was performed by BGSU's Cybersecurity team in 2019
  - External Penetration test was performed by Campus Guard Spring of 2021

- **Security Assessment Requirements (3.12): Assess security controls periodically and implement action plans**
  - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems
  - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems

- **System and Communications Protection Requirements (3.13): Monitor, control, and protect organizational communications**
  - Protect the authenticity of communications sessions
    - SFP records for email
    - Encrypted email while transmitting nonpublic personal information

- **System and Information Integrity Requirement (3.14): Identify, report, and correct information flaws in a timely manner**
  - From a systems side, we monitor regularly and address immediately
  - Receive and review Cybersecurity and Infrastructure Security Agency vulnerability security bulletins and update systems as appropriate
  - Office of Financial Aid and Office of Student Accounts handle process deficiencies

Oversee service providers

Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for Federal Student Aid, student, and school (customer) information at issue.

The following are among the third party service providers used by the college. The activities may include collection of data, transmission of documents, transfers of funds, or other similar services.

- Award Management (Scholarship Management System)
- BankMobile (Customers Bank)
- EdFinancial Services, LLC
- Follett (Bookstore Services)
- Nelnet (Payment Gateway and Processing Services)
- National Student Clearinghouse

Requiring your service providers by contract to implement and maintain such safeguards.

- The college has a contract review process which is used to review service providers' safeguards
- ITS requires all cloud based vendors to conduct a security review (**Appendix B**) prior to signing a contract. (HECVAT)

Evaluate and adjust the information security program based on the results of testing and monitoring, changes to operations or business practices, or other circumstances with a material impact on the information security program.

As part of the overall Information Security Management System, Information Technology Services routinely researches for new vulnerabilities, monitors the network for attacks and annually conducts a variety of Information Technology audit against our systems. The overall information security program is periodically evaluated and adjusted to reflect changing college business, measurements of program effectiveness, and lessons learned from the implementation of security safeguards.

Appendix A: Incident Response Plan Overview

Owens Information Technology Services Office has established a formal incident response plan. The following is the first two sections providing an overview. For a complete copy of the plan, please contact the Owens Information Technology Services Office.

Introduction

Owens Information Technology (IT) systems are fundamental to business operations, and any problem affecting technological resources can quickly impact the business. Responding efficiently and effectively to security incidents is crucial for minimizing risks to the college and its students, faculty, staff, and alumni. Therefore, Owens has developed a Computer Security Incident Response Plan (CSIRP), along with an incident response team, to effectively respond to security events.

Purpose

The purpose of this plan is to provide organizational structure, operational structure, processes, and procedures to Owens personnel, such that they can properly respond to incidents that may affect the function and security of IT assets, information resources, and college operations.

It has been created to provide a functional working document that will assist Owens in identifying, managing, investigating, and remediating various incidents. The CSIRP is intended as functional plan that describes the processes for implementing a response, and also as a guide for establishing the structure needed during incidents as they occur. This document will also reference and provide direction to other procedural documentation that provides operational-level details specific to handling the various incident types.

It is recognized that the CSIRP cannot anticipate and provide guidance for all potential incidents. Management and incident responders should consider the current situation, college impact, and security needs of Owens and balance those against the guidance and recommendations provided by the CSIRP.

Appendix B: Cloud Security Assessment

Due to the strategic direction of Owens, utilizing cloud based systems is expanding. Utilizing cloud based resources relinquishes traditional controls, however they can be mitigated through due diligence in evaluating, documenting and contract wording. The following is a summary used by Owens. For a complete copy of the plan, please contact the Owens Information Technology Services Office.

Shared Assessments Introduction

Campus IT environments are rapidly changing and the speed of cloud service adoption is increasing. Institutions looking for ways to do more with less see cloud services as a good way to save resources. As campuses deploy or identify cloud services, they must ensure the cloud services are appropriately assessed for managing the risks to the confidentiality, integrity and availability of sensitive institutional information and the PII of constituents. Many campuses have established a cloud security assessment methodology and resources to review cloud services for privacy and security controls. Other campuses don't have sufficient resources to assess their cloud services in this manner. On the vendor side, many cloud services providers spend significant time responding to the individualized security assessment requests made by campus customers, often answering similar questions repeatedly. Both the provider and consumer of cloud services are wasting precious time creating, responding, and reviewing such assessments.

The Higher Education Cloud Vendor Assessment Tool attempts to generalize higher education information security and data protection questions and issues for consistency and ease of use. Some institutions may have specific issues that must be addressed in addition to the general questions provided in this assessment. It is anticipated that this Higher Education Cloud Vendor Assessment Tool will be revised over time to account for changes in cloud services provisioning and the information security and data protection needs of higher education institutions.

The Higher Education Cloud Vendor Assessment Tool:

- *Helps higher education institutions ensure that cloud services are appropriately assessed for security and privacy needs, including some that are unique to higher education*

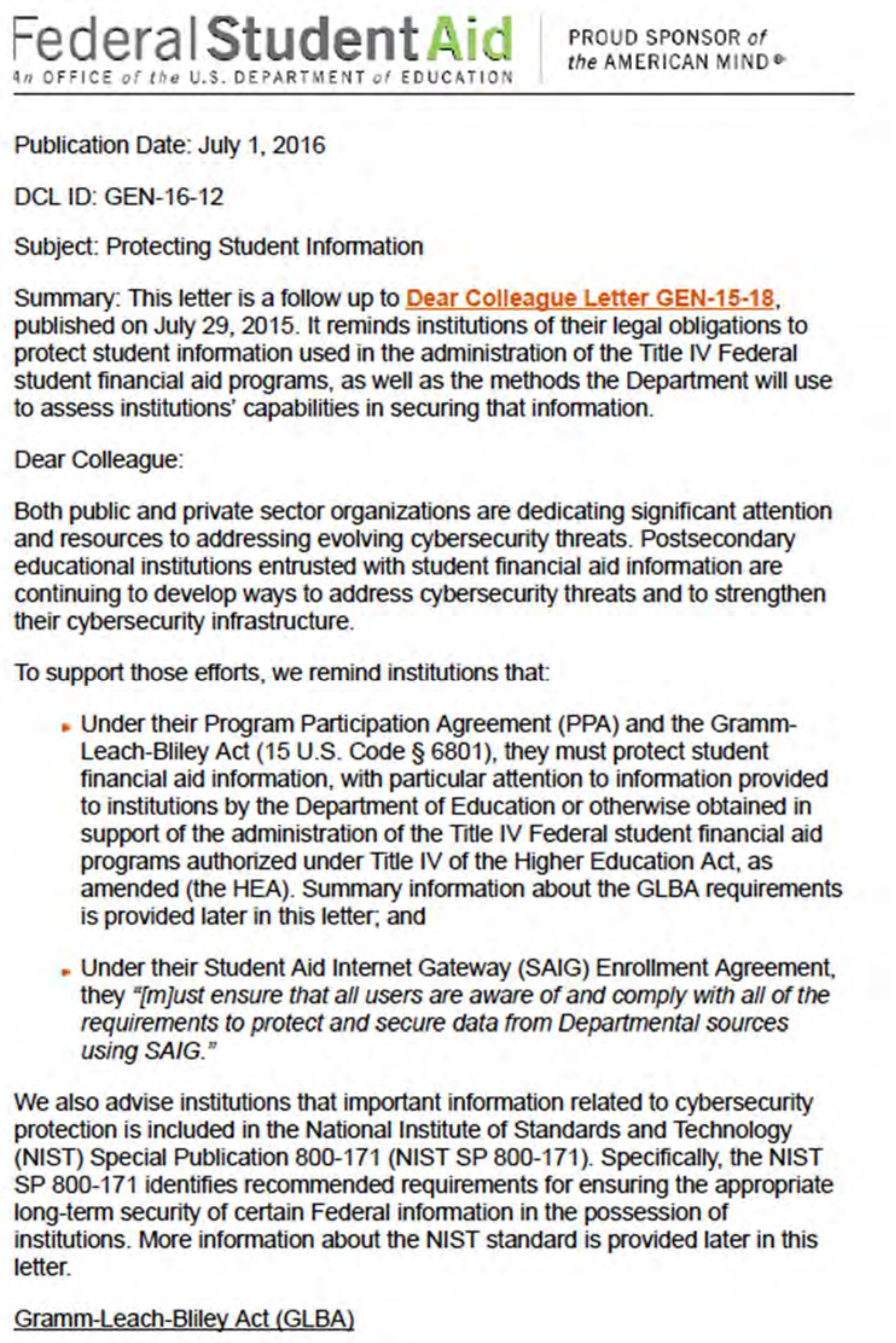
- *Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through cloud services without increasing risks*

- *Reduces the burden that cloud service providers face in responding to requests for security assessments from higher education institutions*

This Higher Education Cloud Vendor Assessment Tool was created by the Higher Education Information Security Council Shared Assessments Working Group. Its purpose is to provide a starting point for the assessment of third-party provided cloud services and resources. Over time, the Shared Assessments Working Group hopes to create a framework that will establish a community resource where institutions and cloud services providers will share completed Higher Education Cloud Vendor Assessment Tool assessments.

This Higher Education Cloud Vendor Assessment Tool is brought to you by the Higher Education Information Security Council, and members from EDUCAUSE, Internet2, and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).

Appendix C: IFAP-Dear Colleague Letter July 2016



Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of
the AMERICAN MIND®

Publication Date: July 1, 2016

DCL ID: GEN-16-12

Subject: Protecting Student Information

Summary: This letter is a follow up to Dear Colleague Letter GEN-15-18, published on July 29, 2015. It reminds institutions of their legal obligations to protect student information used in the administration of the Title IV Federal student financial aid programs, as well as the methods the Department will use to assess institutions' capabilities in securing that information.

Dear Colleague:

Both public and private sector organizations are dedicating significant attention and resources to addressing evolving cybersecurity threats. Postsecondary educational institutions entrusted with student financial aid information are continuing to develop ways to address cybersecurity threats and to strengthen their cybersecurity infrastructure.

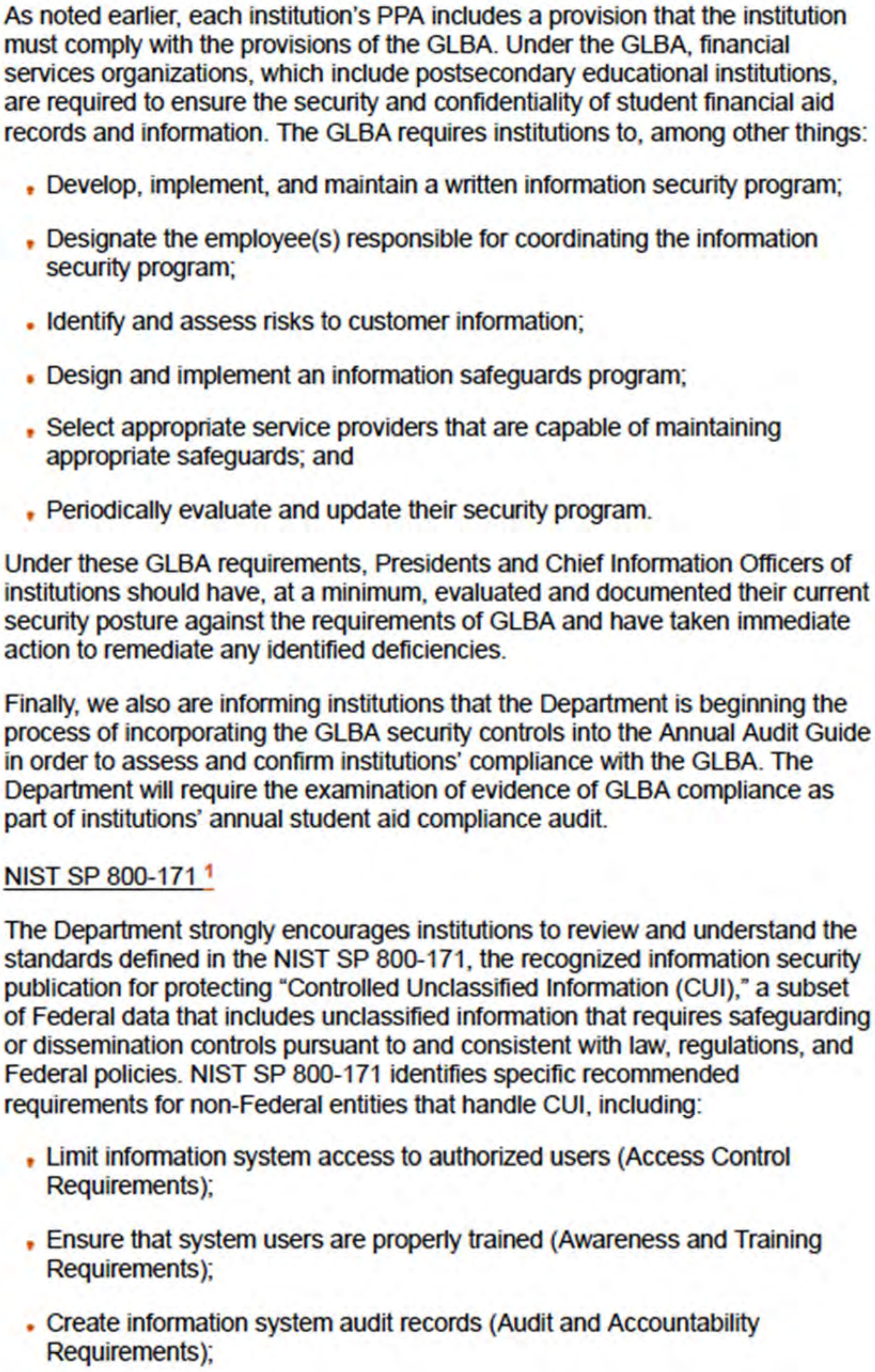
To support those efforts, we remind institutions that:

- Under their Program Participation Agreement (PPA) and the Gramm-Leach-Bliley Act (15 U.S. Code § 6801), they must protect student financial aid information, with particular attention to information provided to institutions by the Department of Education or otherwise obtained in support of the administration of the Title IV Federal student financial aid programs authorized under Title IV of the Higher Education Act, as amended (the HEA). Summary information about the GLBA requirements is provided later in this letter; and

- Under their Student Aid Internet Gateway (SAIG) Enrollment Agreement, they *"[m]ust ensure that all users are aware of and comply with all of the requirements to protect and secure data from Departmental sources using SAIG."*

We also advise institutions that important information related to cybersecurity protection is included in the National Institute of Standards and Technology (NIST) Special Publication 800-171 (NIST SP 800-171). Specifically, the NIST SP 800-171 identifies recommended requirements for ensuring the appropriate long-term security of certain Federal information in the possession of institutions. More information about the NIST standard is provided later in this letter.

Gramm-Leach-Bliley Act (GLBA)



As noted earlier, each institution's PPA includes a provision that the institution must comply with the provisions of the GLBA. Under the GLBA, financial services organizations, which include postsecondary educational institutions, are required to ensure the security and confidentiality of student financial aid records and information. The GLBA requires institutions to, among other things:

- Develop, implement, and maintain a written information security program;
- Designate the employee(s) responsible for coordinating the information security program;
- Identify and assess risks to customer information;
- Design and implement an information safeguards program;
- Select appropriate service providers that are capable of maintaining appropriate safeguards; and
- Periodically evaluate and update their security program.

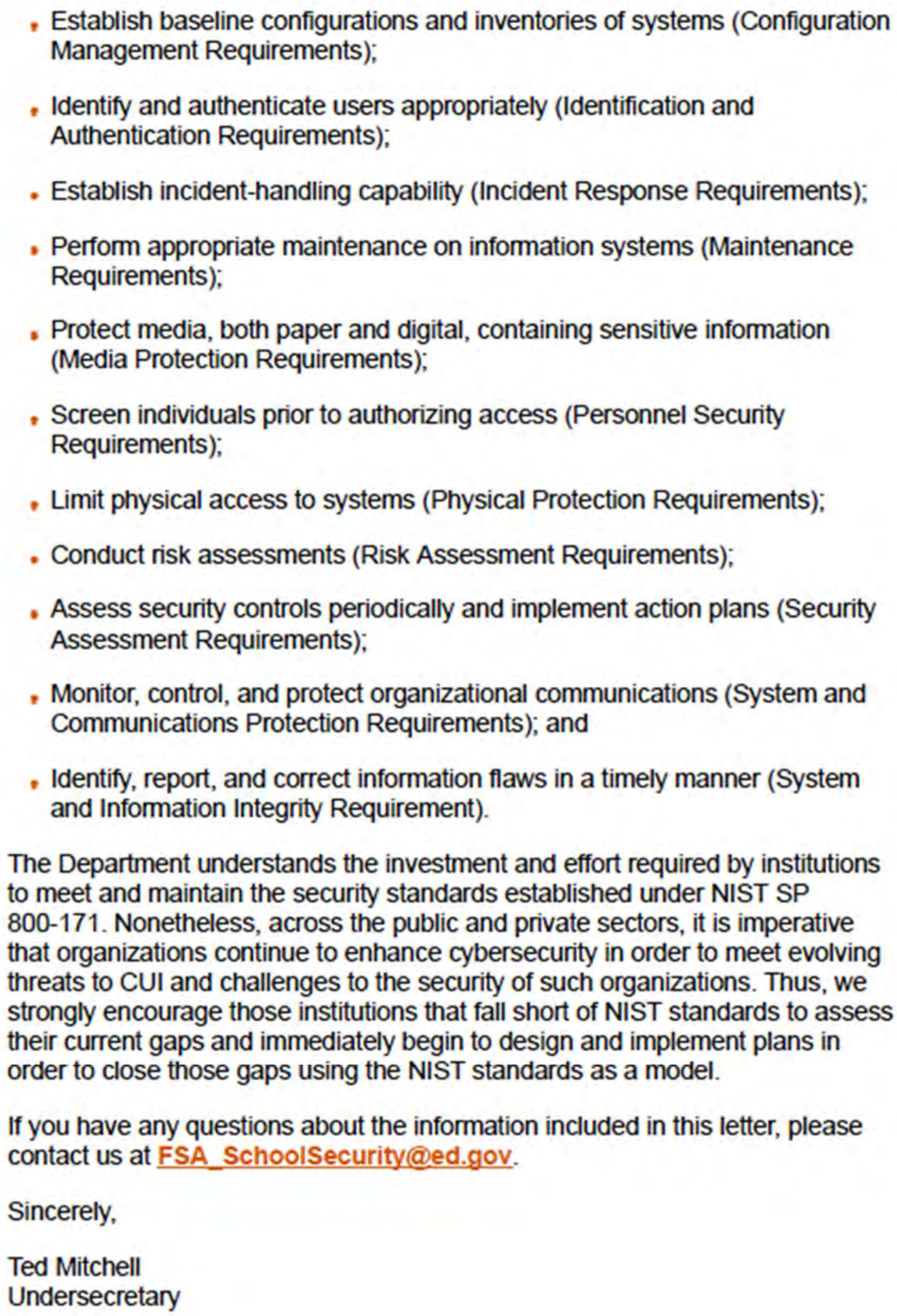
Under these GLBA requirements, Presidents and Chief Information Officers of institutions should have, at a minimum, evaluated and documented their current security posture against the requirements of GLBA and have taken immediate action to remediate any identified deficiencies.

Finally, we also are informing institutions that the Department is beginning the process of incorporating the GLBA security controls into the Annual Audit Guide in order to assess and confirm institutions' compliance with the GLBA. The Department will require the examination of evidence of GLBA compliance as part of institutions' annual student aid compliance audit.

NIST SP 800-171 [1]

The Department strongly encourages institutions to review and understand the standards defined in the NIST SP 800-171, the recognized information security publication for protecting "Controlled Unclassified Information (CUI)," a subset of Federal data that includes unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Federal policies. NIST SP 800-171 identifies specific recommended requirements for non-Federal entities that handle CUI, including:

- Limit information system access to authorized users (Access Control Requirements);
- Ensure that system users are properly trained (Awareness and Training Requirements);
- Create information system audit records (Audit and Accountability Requirements);



- Establish baseline configurations and inventories of systems (Configuration Management Requirements);
- Identify and authenticate users appropriately (Identification and Authentication Requirements);
- Establish incident-handling capability (Incident Response Requirements);
- Perform appropriate maintenance on information systems (Maintenance Requirements);
- Protect media, both paper and digital, containing sensitive information (Media Protection Requirements);
- Screen individuals prior to authorizing access (Personnel Security Requirements);
- Limit physical access to systems (Physical Protection Requirements);
- Conduct risk assessments (Risk Assessment Requirements);
- Assess security controls periodically and implement action plans (Security Assessment Requirements);
- Monitor, control, and protect organizational communications (System and Communications Protection Requirements); and
- Identify, report, and correct information flaws in a timely manner (System and Information Integrity Requirement).

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.

If you have any questions about the information included in this letter, please contact us at FSA_SchoolSecurity@ed.gov.

Sincerely,

Ted Mitchell
Undersecretary