UNITED STATES DEPARTMENT OF EDUCATION

THE UNDER SECRETARY

GEN-16-12 July 1, 2016

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:

[1] A copy of NIST SP 800-171 is available free of charge at http://dx.doi.org/10.6028/NIST.SP.800-171.

- 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

Ted Mitchell
Undersecretary