Education Department Highlights Enforcement of GLBA Cybersecurity Requirements and Potential Penalties

By Allison Davis, Partner, CapinTech and Lisa Saul, Partner, CapinCrouse

The United States Education Department (ED) has released another memo related to the Student Financial Assistance program, specifically focused on postsecondary and third-party service organizations' requirements to comply with the Gramm-Leach-Bliley Act (GLBA) and the potential consequences of noncompliance.

Key Takeaways

The memo notes that:

- Noncompliance with GLBA could result in a breach of the Program Participation Agreement (PPA) and a finding in the audit report.
- The Federal Student Aid (FSA) Postsecondary Institution Cybersecurity Team will be informed of any findings and may request additional information to assess the level of risk**.**
- **If it is determined that substantial risk to the security of the information exists, the Cybersecurity Team may disable access to the ED's information systems or recommend a fine or other administrative action.**

GLBA Considerations

Institutions participating in the FSA program have agreed to comply with GLBA as part of the Program Participation Agreement with the ED. The goal is to ensure the confidentiality, security, and integrity of student and parent information gathered as a result of FSA programs.

While GLBA is not new guidance, the compliance of these postsecondary institutions with GLBA is becoming scrutinized by auditors as part of the Uniform Guidance audits.

Under the 2019 compliance supplement effective for fiscal year ends June 30, 2019 through May 31, 2020, auditors are required to evaluate the following three components of GLBA:

- Has the institution designated an individual to coordinate its information security program?
- Has the institution performed a risk assessment that evaluates the risks to student and parent information? The risk assessment should address, at a minimum, risks related to these areas:
  - 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 system failures
- Are risks and their mitigating safeguards documented?

While only a few components of GLBA are included in audit testing under the 2019 compliance supplement effective for fiscal year ends June 30, 2019 through May 31, 2020, institutions have attested to full compliance with GLBA as part of their PPA. **Therefore, it's imperative to ensure your institution is in compliance or, at a minimum, actively working toward compliance with a documented timeline and plan.**

It's also important to note that even if the GLBA requirements don't apply to your institution, they can help reduce your cybersecurity risk.

CapinTech, a CapinCrouse company, has been helping organizations comply with GLBA for over 20 years. Please contact us as cybersecurity@capincrouse.com to discuss how we can assist your institution or to request a sample risk assessment plan template.

(continued)

Additional Resources:

The Gramm-Leach-Bliley Act: What Higher Education Institutions Need to Do Now

5 Steps to Strengthen Your Institution's Cybersecurity Defenses

CapinTech Cyber Fitness Self-Test

How to Develop an Effective IT Audit Program

Cybersecurity Training: Who, What, When, Where, and Why

About the Authors

Allison Davis, Partner
CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

Lisa Saul, Partner
Uniform Guidance Director
lsaul@capincrouse.com
o 505.50.CAPIN ext. 2050

Lisa joined CapinCrouse in 1999. She has over 20 years of experience in performing and supervising Uniform Guidance audits of Department of Education student financial aid programs and a variety of federal funding, as well as program audits and agreed-upon procedure engagements of various state-funded programs. Lisa oversees the firm's more than 80 Uniform Guidance audits.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.