Agency Priority Goal Action Plan

Improve Student Privacy and Data Security at Institutions of Higher Education (IHEs) through Outreach and Compliance Efforts

Goal Leader: Jason Gray, Chief Information Officer, Office of the Chief Information Officer

Deputy Goal Leader: Michael Hawes, Director of the Student Privacy Policy and Assistance Division, Office of the Chief Privacy Officer, Office of Management

Performance.gov

Fiscal Year 2018, Quarter 3

Overview

Goal Statement

- By September 30, 2019, the Department will increase information security program outreach activities to institutions of higher education (IHEs) by 40% in order to help protect IT systems and data privacy and commence audits of IHEs subject to A-133 and Gramm-Leach-Bliley Act (GLBA), resulting in 36 IHEs (from a baseline of zero) completing an audit of GLBA-related information security safeguards with no significant findings.

Challenge

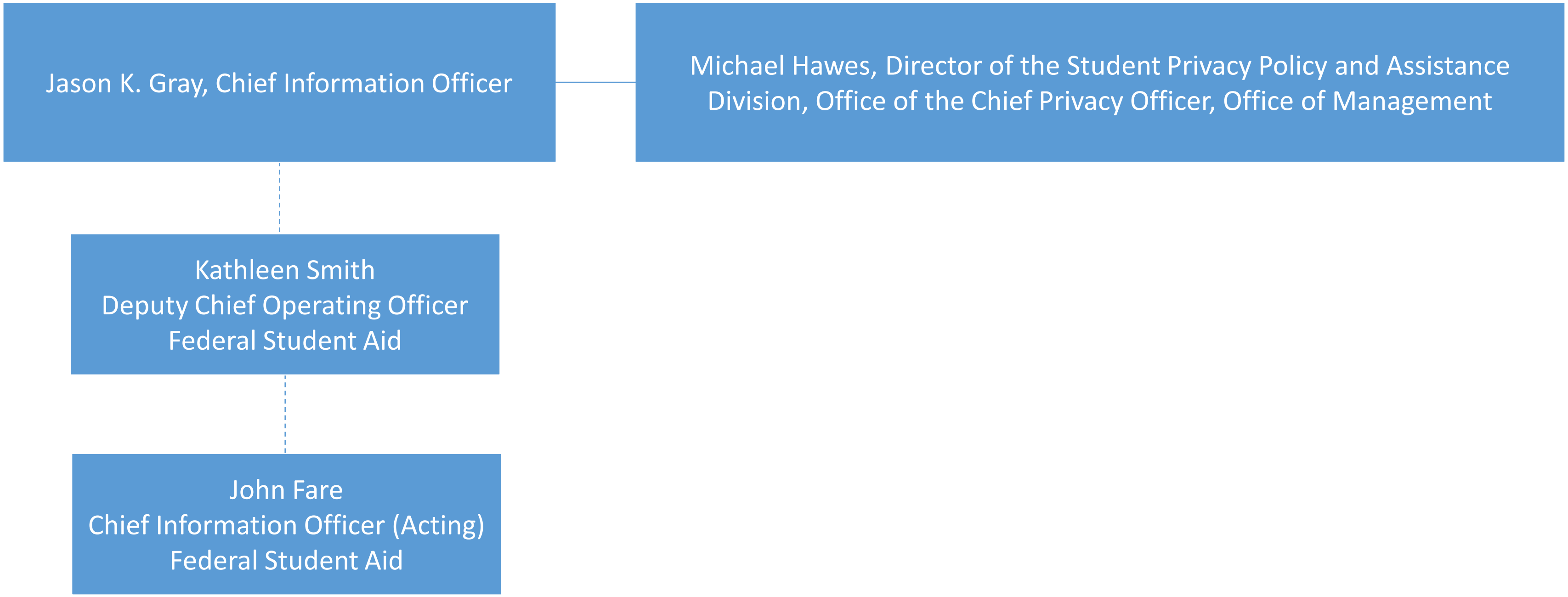
- Available data suggests IHEs are increasingly becoming targets of cyber-attacks and potentially placing ED data and the efficacy of systems and programs at risk;
- Many IHEs do not adequately understand the magnitude of the threat to student data, the actions that need to be taken to protect student privacy, nor the urgency with which the Department views this matter; and
- IHE leadership is not always fully aware of their responsibilities for self-reporting, and therefore, fail to engage with the Department in a timely fashion to self-report and are slow to respond to the Department's inquiries.

Opportunity

- Significant opportunities for collaboration already exist and can be built upon, including conferences, industry meetings, and agency-initiated trainings.

Leadership

Visual representation of the goal team governance structure:



Jason K. Gray, Chief Information Officer

Michael Hawes, Director of the Student Privacy Policy and Assistance Division, Office of the Chief Privacy Officer, Office of Management

Kathleen Smith
Deputy Chief Operating Officer
Federal Student Aid

John Fare
Chief Information Officer (Acting)
Federal Student Aid

Goal Structure & Strategies

The Department will achieve this APG through collaborative efforts involving training, outreach, monitoring, and reporting.

- An IHE outreach strategy related to GLBA compliance has been developed and an outreach timeline constructed.
- The number of IHEs passing an audit of GLBA-related information security safeguards. Such safeguards including designating responsible individuals to coordinate the security program, obtaining IHE risk assessment, and obtaining the documentation created by the IHE that aligns each safeguard with each risk.*
- Outreach activities carried out by Federal Student Aid (FSA) and the Privacy Technical Assistance Center (PTAC) related to privacy and data security requirements is ongoing.
- Tracking timely privacy and data security reports received by FSA from recipients of outreach activities as a result of FSA's outreach activities.

*Timing of the issuance of new audit standards for GLBA-related information security safeguards, to be published in the OMB Compliance Supplement, could impact the requirement of IHEs to conduct and submit an audited assessment of data security programs.

Summary of Progress – FY 18 Q3

- Privacy Technical Assistance Center (PTAC) and Federal Student Aid (FSA) surpassed target of 14 training sessions; 59 sessions (9 sessions in Quarter 1, 9 in Quarter 2 and 31 in Quarter 3) provided privacy and data security requirements to IHEs, their education associations and other target audiences.
- FSA is evaluating the proposed audit standards for GLBA-related information security safeguards to be published in the OMB Compliance Supplement. Issuance was postponed for 2018.
- FSA met with the American Council on Education (ACE) and EDUCAUSE, a leading policy advocacy body for information technology in higher education, regarding initial discussion of a Postsecondary Institution (PSI) Breach Process. Further discussion of this process will continue into Quarter 4.

Next Steps:

- FSA is completing the reengineering of the PSI Breach Process to increase the transparency, the responsiveness, and the inclusion of PSI's in a cooperative partnership to address potential PII breaches.

Key Milestones

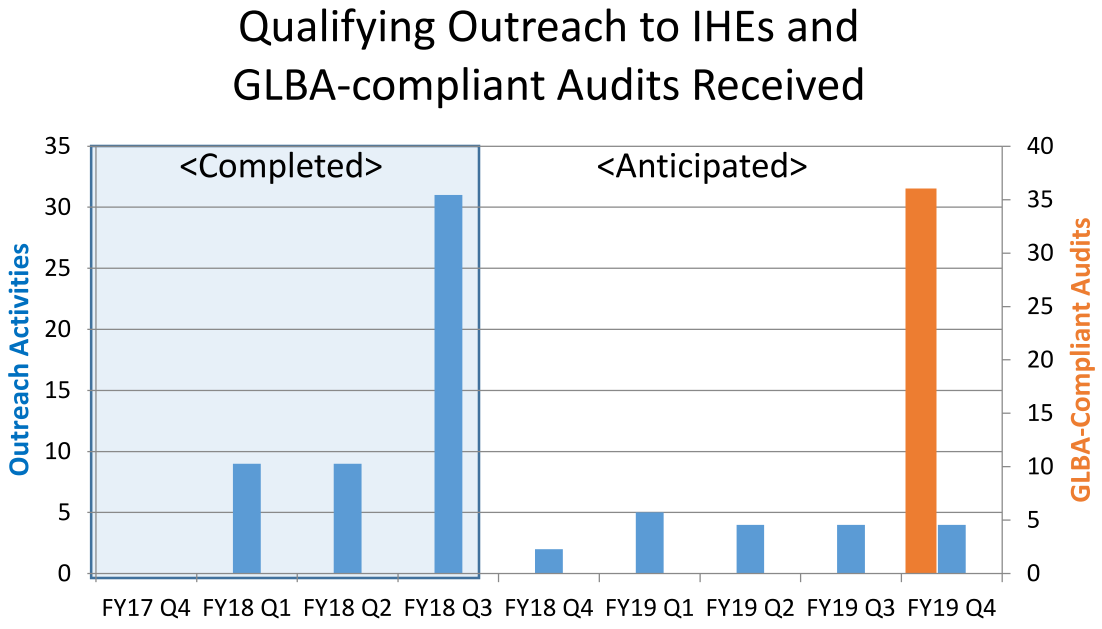
The milestones on the path to achieving this APG include activities around outreach, technical assistance, and monitoring/tracking.

Milestone Summary					
Key Milestone	**Milestone Due Date**	**Milestone Status**	**Change from last quarter**	**Owner**	**Comments**
In FY 2018, FSA will work closely with OMB and IHEs to prepare for the upcoming GLBA audit guidance.*	FY 2018	Not Met	0	Michael Hawes/ John Fare	Publication of GLBA audit requirements in the FY 2018 OMB Compliance Supplement was postponed.* FY 2019 publication is on-track.
In FY 2018, 14 outreach activities targeting privacy and data security requirements will be performed at/for IHEs by FSA.	FY 2018	Target Exceeded	+31	Michael Hawes/ John Fare	Outreach opportunities continue and the Department surpassed its FY 2018 performance target in March 2018.
In FY 2019, at least 36 IHEs will have an audit of GLBA-related information security safeguards which result in no significant findings .	FY 2019			Michael Hawes/ John Fare	
In FY 2019, 17 outreach activities targeting privacy and data security requirements will be performed at/for IHEs by FSA.	FY 2019			Michael Hawes/ John Fare	
In FY 2020, at least 77 IHEs will have an audit of GLBA-related information security safeguards which result in no significant findings.	FY 2020			Michael Hawes/ John Fare	
In FY 2020, 20 outreach activities targeting privacy and data security requirements will be performed at/for IHEs by FSA .	FY 2020			Michael Hawes/ John Fare	

*Timing of the issuance of new audit standards for GLBA-related information security safeguards, to be published in the OMB Compliance Supplement, impacts the requirement of institutions to conduct and submit an audited assessment of data security programs.

Key Indicators

Although the Department has conducted outreach in the past, FY 2018 will be the first year the Department has systematically tracked this type of outreach.



The Department will increase information security program outreach activities to IHEs and commence audits of IHEs, subject to A-133 and Gramm-Leach-Bliley Act (GLBA), completing an audit of GLBA-related information security safeguards. Of the thousands of audits that will be conducted, the Department anticipates a minimum of 36 IHEs (from a baseline of zero) completing an audit of GLBA-related information security safeguards with no significant findings.

A baseline of zero for FY17 Q4 represents a new, updated definition of qualifying outreach activities.

Data Accuracy and Reliability

Each metric has a unique data source.

For the audit metric (a) the data source is IHE-provided auditor reports accessed and analyzed by FSA and the Education Privacy Technical Assistance Center. Data accuracy will be subject to the limitation of data timeliness – due to input being created from auditor reports.

For outreach metric (b) the activity records maintained by the FSA are on a secure SharePoint site. As each activity is completed by FSA or the Department’s Privacy Technical Assistance Center, it will be recorded in the SharePoint site. Data accuracy will be high, reliable and consistent, based on contractor, ED personnel and FSA personnel actions. The SharePoint site has been created and is ready for data input. Limitations include entry error and individual bandwidth.

Additional Information

Contributing Programs

Organizations:

- Institutions of Higher Education (IHE)
- Office of Federal Student Aid
- The Department’s Office of the Chief Information Officer
- The Department of Education's Office of the Chief Privacy Officer

Program Activities:

- Enhanced outreach to higher education institutions
- Audits of GLBA-related information security safeguards at higher education institutions

Regulations:

- OMB Circular A-133 and A-133 Compliance- serves to identify existing important compliance requirements that the Federal Government expects to be considered as part of an audit required by the 1996 Amendments.
- Gramm-Leach-Bliley Act (GLBA) Safeguards Audits check for the following:

  a. Verify that the IHE has designated an individual to coordinate the information security program.

  b. Obtain the IHE risk assessment and verify that it addresses the three required areas noted in GLBA 16 CFR 314.4 (b).

  c. Obtain the documentation created by the IHE that aligns each safeguard with each risk identified from step b above, verifying that the IHE has identified a safeguard for each risk.

Stakeholder Consultation

Stakeholder feedback has included, but is not limited to, the American Institute of Certified Public Accountants (AICPA), EDUCAUSE, ACE, the National Association of Student Financial Aid Administrators and attendees of the Annual FSA Training Conference.