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

Overview

Goal Statement

- By September 30, 2019, the Department of Education (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
  - Begin 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

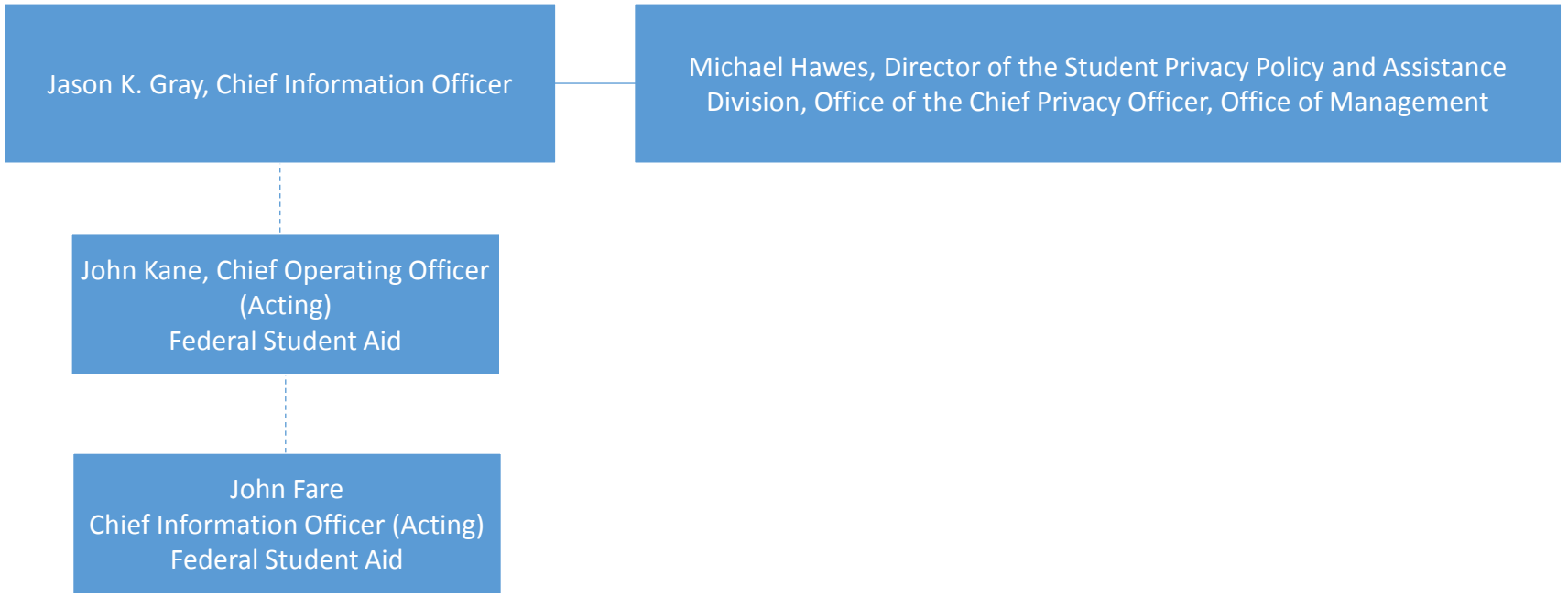
- Available data suggest that IHEs are increasingly becoming targets of cyber-attacks and potentially placing Department data and the efficacy of systems and programs at risk;
- Many IHEs may not appreciate the magnitude of the threat to student data, the actions needed to protect student privacy, nor the urgency with which the Department views this matter; and
- IHE leadership may not be fully aware of their responsibilities for self-reporting cyber-incidents, and therefore, fail to inform the Department and respond to any inquiries in a timely fashion.

Opportunity

- 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:



Goal Structure & Strategies

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

- 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 include 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.*
- Ongoing outreach activities by Federal Student Aid (FSA) and the Privacy Technical Assistance Center (PTAC) related to privacy and data security requirements.
- Tracking the timeliness of privacy and data security reports received by FSA as a result of FSA outreach activities.

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

Summary of Progress – FY 18 Q4

- Privacy Technical Assistance Center (PTAC) and Federal Student Aid (FSA) surpassed FY 2018 target of 14 training sessions; 63 sessions provided privacy and data security requirements to Institutes of Higher Education (IHE), their education associations and other target audiences.
- FSA established processes for GLBA compliance audit reviews. Similar to current procedures, the A-133 audit conducted at IHEs will be reviewed by FSA, to include the GLBA audit area, in the coming FY 2019 cycle. If noncompliance is found by the external auditor, this information will be relayed to the Federal Trade Commission (FTC) for review and appropriate action. Next year's data will establish a baseline for potential audit findings.

Next Steps:

- Publish audit procedures as part of the FY 2019 OMB A-133 Compliance Supplement.
- Continue to conduct outreach activities, to include a possible electronic announcement addressing the GLBA compliance audit requirement.
- Monitor incoming audits for GLBA compliance and follow established processes for referring areas of noncompliance to the FTC.

Key Milestones

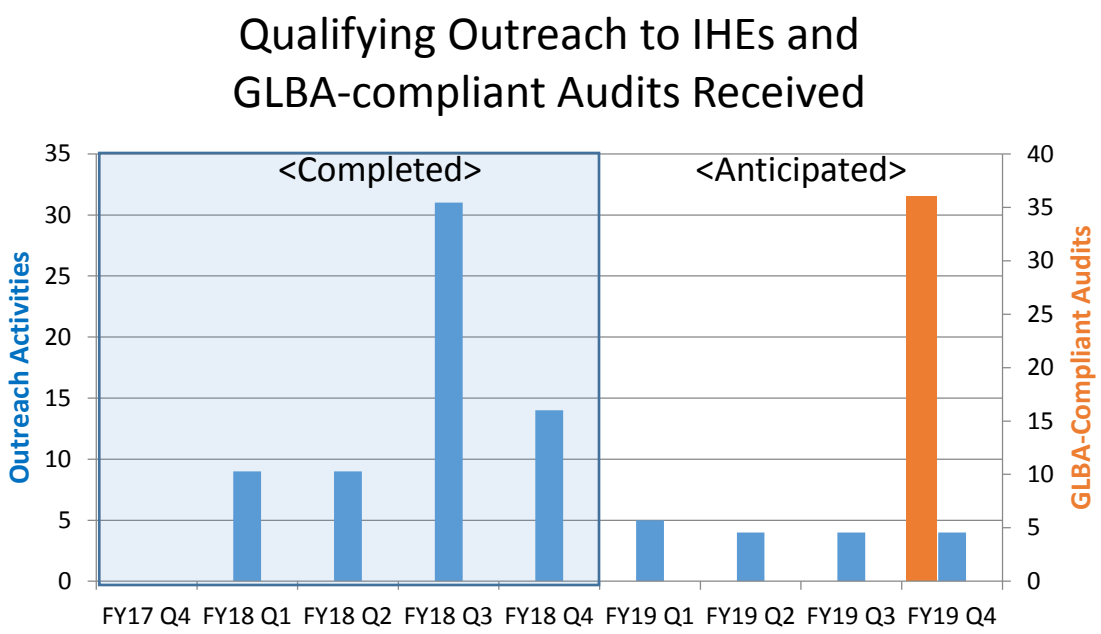
The milestones on the path to achieving this APG include activities around outreach, technical assistance, and monitoring/tracking.

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	63	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	

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

Key Indicators

Although the Department has conducted outreach in the past, FY 2018 was the first year the Department has systematically tracked this 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 the new, updated definition of qualifying outreach activities.

Data Accuracy and Reliability

Each metric has a unique data source.

For the outreach metric, 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 a SharePoint site. Based on contractor, Department personnel and FSA personnel actions, data accuracy will be high, reliable and consistent. The SharePoint site has been created and is ready for data input. Limitations include entry error and staff resources.

For the audit metric, the data source is IHE-provided auditor reports accessed and analyzed by FSA and the Privacy Technical Assistance Center. Due to input being created from auditor reports, data accuracy will be subject to the limitation of data timeliness.

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'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 identify existing Federal compliance requirements to be considered as part of an audit as required by the 1996 Amendments.
- Gramm-Leach-Bliley Act (GLBA) Safeguards Audits verify that IHEs have:
  a. Designated an individual to coordinate the information security program.
  b. Addressed the three required areas noted in GLBA 16 CFR 314.4 (b) in their risk assessments.
  c. 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.