Agency Priority Goal (APG) Action Plan

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

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

APG Deputy Goal Leader: Jessica Ramakis, Acting Director of the Student Privacy Policy Office, Office of Planning, Evaluation and Policy Development

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
  - Commence audits of IHEs subject to the Single Audit* 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.

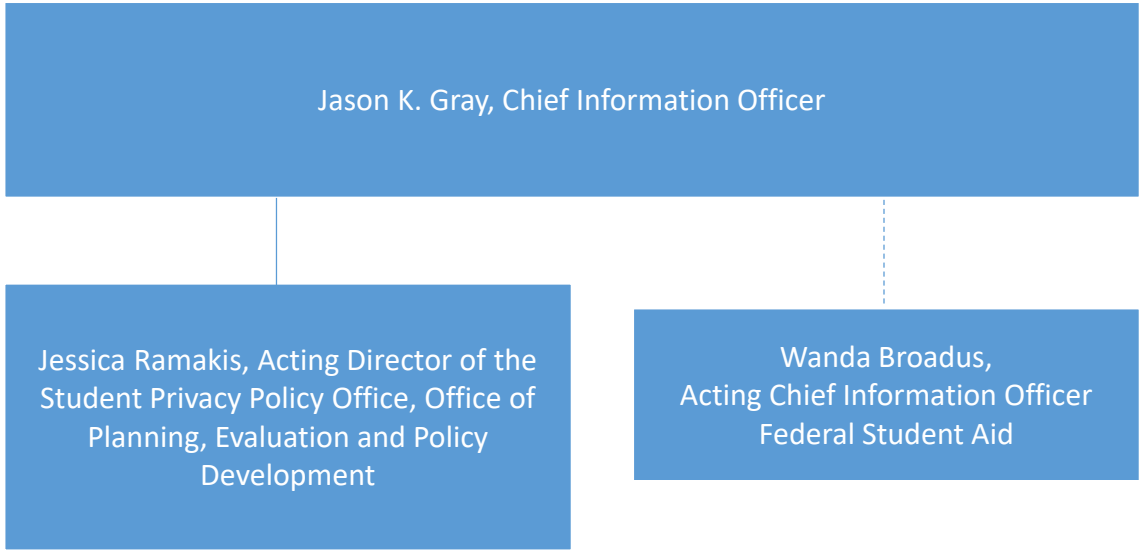
Opportunity

- Collaboration already exist and can be built upon, including conferences, industry meetings, and agency-initiated trainings.

*Previously known as OMB Circular A-133.

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, performing a risk assessment, and documenting a safeguard for each risk identified.*
- Ongoing outreach activities by Federal Student Aid (FSA) and the Privacy Technical Assistance Center (PTAC) within the Student Privacy Policy Office (SPPO) 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 were published in the June 2019 2 C.F.R. Part 200 Appendix IX Compliance Supplement (Compliance Supplement) and impact the requirement of IHEs to conduct and submit an audited assessment of data security programs.

Summary of Progress – FY 2019 Q4

- In Quarter 4, FSA made 585 cybersecurity-related contacts with IHEs. Of note, 238 were related to an Inspector General memo for a specific software vulnerability. FSA conducted data calls, exchanged threat information, and discussed best practices during these engagements. FSA worked with IHEs and tracked the remediation actions, including IHEs completing the remediation and patching actions.
- FSA and the SPPO, through the PTAC, continued assisting IHEs by delivering outreach activities focused on data privacy and security. Although the FY 2019 target had been met as of Quarter 2, 17 new outreach activities were delivered in Quarter 4.
- The Department collaborated with higher education associations to work on strengthening the Department's common understanding of IHE protections for participants in the Title IV programs. The engagements have produced a series of common objectives in areas such as defining the term "breach," security compliance frameworks, and how the Department will engage Title IV program participants in the future. OCIO established the foundation for increased collaboration and information sharing to achieve common understanding that will enable the sharing of operational threat information, best practices, and effects of changing technologies and policies to inform efforts within the Department and across IHEs.

Summary of Progress – FY 2018 through FY 2019

- In FY 2019, the Department focused on collaborative efforts involving training, outreach, monitoring, and reporting. New audit standards for GLBA-related information security safeguards were published in the June 2019 2 C.F.R. Part 200 Appendix IX Compliance Supplement and impact the requirement of IHEs to conduct and submit an audited assessment of data security programs. IHEs subject to the Single Audit have nine months from their fiscal year end to submit the audits to the Department; IHEs will not include the newly required standards in time to meet the Department's FY 2019 APG target.
- In response to the delayed GLBA guidance, in Quarter 3 and Quarter 4 of FY 2019, FSA engaged with 708 IHEs for technical assistance. FSA's contact with these institutions consisted of discussing industry best practices, mitigation strategies, guidance for improving processes, and documentation to improve their security postures.
- In FY 2019, the Department initiated a collaborative engagement with higher education associations. As a result of ongoing dialog, the Department has been able to identify strategic, tactical and operational opportunities for collaboration with IHEs and higher education associations. The Department is defining specific outcomes, sequences of events and proper stakeholder engagement.

The Department achieved this APG in part.

- By September 30, 2019, the Department proposed to increase information security program outreach activities to IHEs by 40% (from a baseline of 12) in order to help protect IT systems and data privacy. From October 2018 through September 2019, FSA and the PTAC surpassed the FY 2018-19 APG target and collaborated to conduct 103 outreach activities targeting data privacy and IT security requirements of IHEs.
- The Department did not meet the target to commence audits of IHEs subject to the Single Audit and GLBA, resulting in 36 IHEs (from a baseline of zero) completing an audit of GLBA-related information security safeguards with no significant findings.

Key Milestones

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

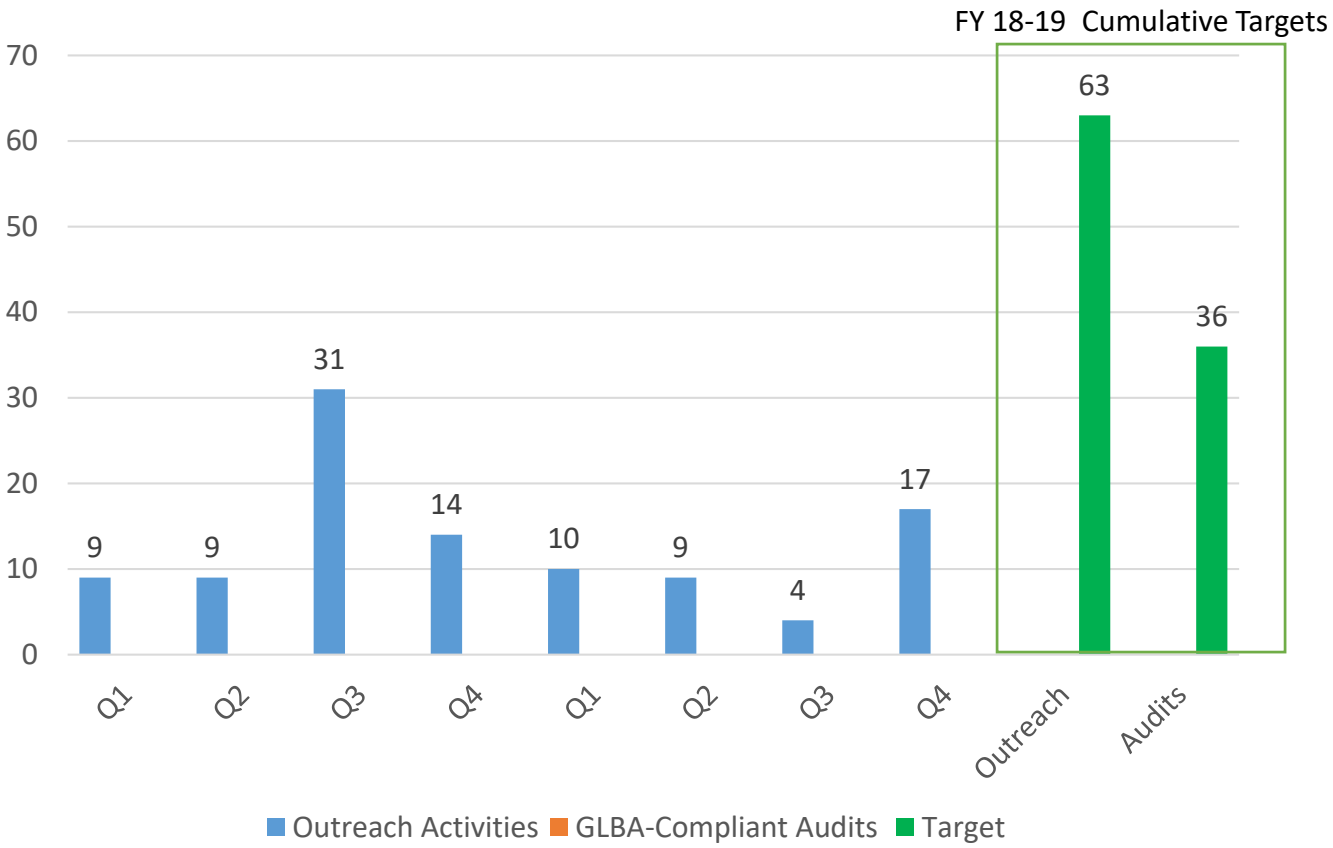
Milestone Summary					
Key Milestone	**Milestone Due Date**	**Milestone Status**	**Change from last quarter**	**Owner**	**Comments**
In FY 2018, FSA will work closely with OMB and IHEs to prepare for the upcoming GLBA audit guidance.*	FY 2018	Not Met	0	Wanda Broadus*	Publication of GLBA audit requirements in the FY 2018 OMB Compliance Supplement was postponed.
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	Jessica Ramakis**/ Wanda Broadus	Outreach opportunities continued 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	Delayed	-	Wanda Broadus	OMB Compliance Supplement that includes GLBA audit requirements was released July 1, 2019. Only Schools with fiscal years ending June 30, 2019, forward will be subject to GLBA testing. Single Audit IHE's have nine months from their fiscal year end to submit the audits to the Department.
In FY 2019, 17 outreach activities targeting privacy and data security requirements will be performed at/for IHEs by FSA and SPPO.	FY 2019	Target Exceeded	4 new activities	Jessica Ramakis/ Wanda Broadus	
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			Wanda Broadus	
In FY 2020, 20 outreach activities targeting privacy and data security requirements will be performed at/for IHEs by FSA and SPPO.	FY 2020			Jessica Ramakis/ Wanda Broadus	

*Wanda Broadus, Acting Chief Information Officer for Federal Student Aid; ** Jessica Ramakis, Acting Director of the Student Privacy Policy Office

7

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 IHEs covered by the Compliance Supplement with fiscal years ending June 30, 2019 forward will have 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.

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. Those activities completed by SPPO through 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.

For the audit metric, the data source is IHE-provided auditor reports accessed and analyzed by FSA. 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 Planning, Evaluation and Policy Development

Program Activities:

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

Statutes:

- The Compliance Supplement identifies existing Federal compliance requirements to be considered as part of an audit as required by the Single Audit Act Amendments of 1996.
- Gramm-Leach-Bliley Act (GLBA) Safeguards Audits determine whether 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, EDUCAUSE, American Council on Education, the National Association of Student Financial Aid Administrators and attendees of the Annual FSA Training Conference.