Agency Priority Goal Action Plan

Student Privacy and Cybersecurity

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

APG Deputy Goal Leader: Kevin Herms, Director of the Student Privacy Policy Office (SPPO), Office of Planning, Evaluation and Policy Development (OPEPD)

Overview

Goal Statement

Impact Statement

- Improve student privacy and cybersecurity at institutions of higher education (IHEs) through outreach and compliance efforts.

Achievement Statement

- By September 30, 2021, the Department will participate in 12 engagements with sector-related non-governmental organizations to inform the development of five best practice programmatic improvements.

Challenge

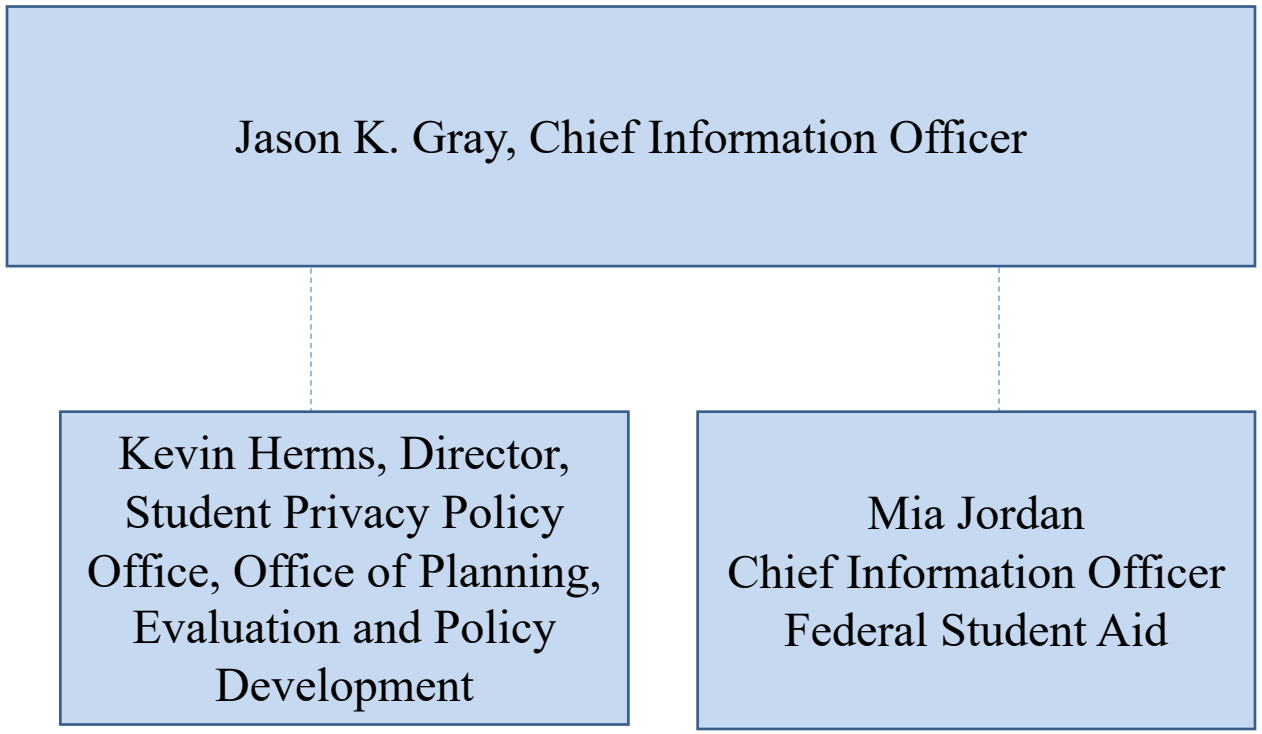
- Available data suggest IHEs are increasingly becoming targets of cyber-attacks and potentially placing Department data and the efficacy of systems and programs at risk.
- Many IHEs may not appreciate the magnitude of the threat to student data, the actions needed to protect student privacy, or the urgency with which the Department views this matter.
- 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 exists and can be built upon, including at conferences, industry meetings and agency-initiated trainings.

Leadership

Visual representation of the goal team governance structure:



Goal Structure & Strategies

This is a two-year Agency Priority Goal (APG) covering FY 2020 and FY 2021.

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

- Issuing best practice programmatic improvements documents to IHEs to provide a definition of information security breach and on when and how to report an information security breach.
- Establishing secure mechanisms for breach notification, including secure storage for such information.
- Creating a process through which IHEs can validate compliance notifications and reporting requests.
- Developing a collaborative IHE outreach strategy related to compliance with the *Gramm-Leach-Bliley Act* (GLBA)* has been developed and an outreach timeline constructed.
- 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 established the requirement of IHEs to conduct and submit an audited assessment of data security programs.

Summary of Progress – FY 2020 Q4

- In Quarter 4, the Institutions of Higher Education (IHE) Cybersecurity Team conducted 37 outreach activities with institutions in response to breach incidents.
  - The Federal Student Aid (FSA) posted a technology security alert electronic announcement on Information for Financial Aid Professionals titled, Ransomware Campaign Targeting Education Institutions. The technology security alert electronic announcement included information on possible vulnerabilities and prevention techniques.
  - The Student Privacy Policy Office (SPPO), through the Privacy Technical Assistance Center, conducted two virtual training activities that included IHEs as part of the target audience. One of these activities was a data breach event, and the second focused on the use of educational applications/educational technology. Through the combined efforts of FSA and SPPO, 56 outreach activities were delivered throughout FY 2020 exceeding the year end goal of 20.
- The Department has collaborated with schools to respond to 160 incidents. Also, the Department provided subject matter expertise with remediation and helped improve the cybersecurity posture for IHE partners.
- Gramm-Leach-Bliley Act outreach and associated school focused activities are on administrative hold to minimize the impact to IHEs operating under the COVID-19 restrictions. The FSA cybersecurity team is preparing notification and corrective action requests for non-compliant schools when the restrictions are lifted.
- Briefed FAME, a commercial service provider in the IHE administrative space, regarding secure cloud and federal resources available to states.

Key Milestones

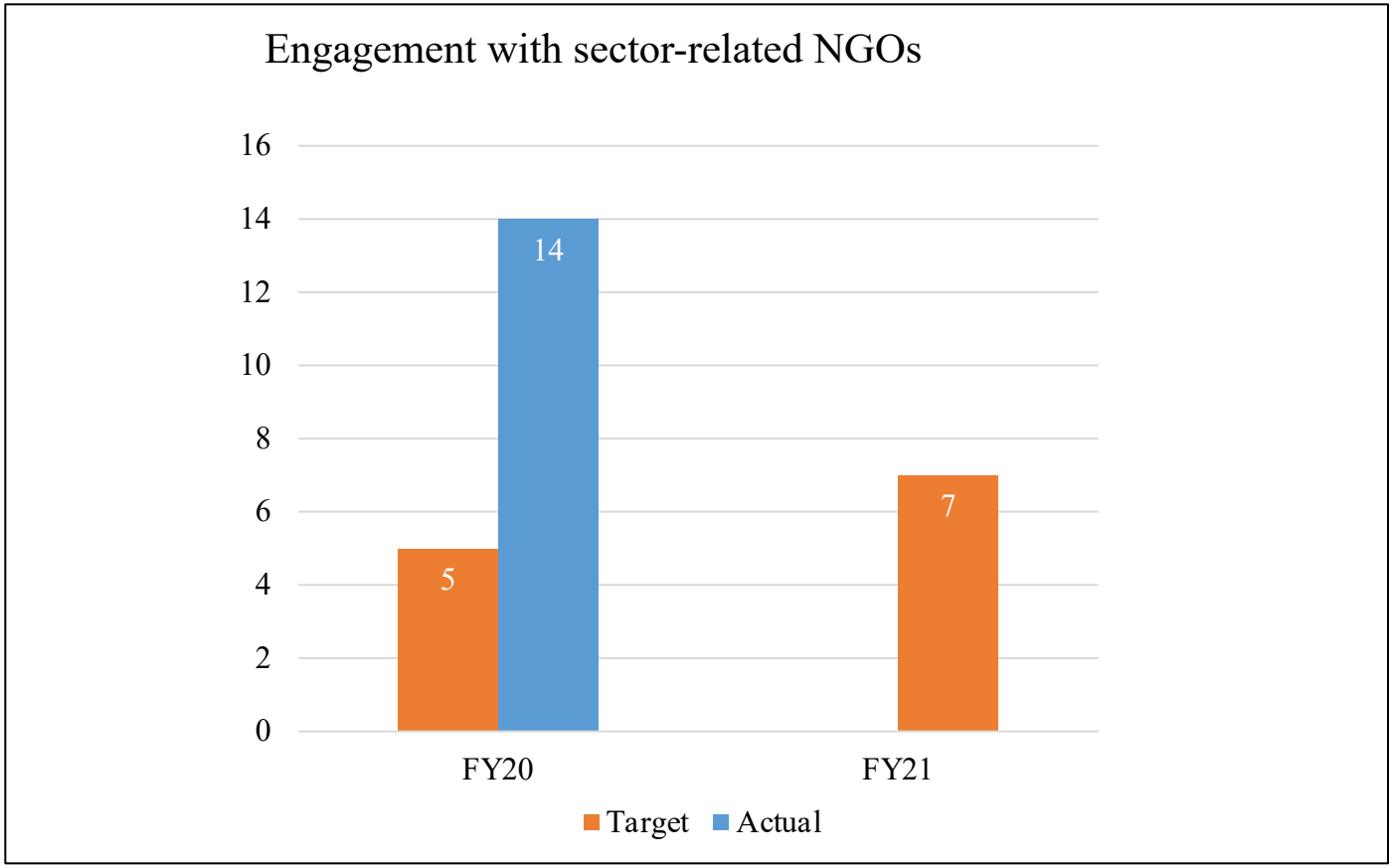
Milestone Summary				
Key Milestone	**Milestone Due Date**	**Milestone Status**	**Owner**	**Comments**
Stakeholder meeting with ED Deputy Secretary to discuss common vision to protect the educational journey for students.		Completed	Jason Gray	Mutual commitment to continue working towards a greater understanding and evolution of security for IHEs. Senior OCIO, FSA and Office of the Secretary (OS) leadership attended.
ED Deputy Secretary meeting with education associations and other groups in the higher education community to discuss institutions' cybersecurity obligations for participation in Title IV federal financial aid programs.		Completed	Jason Gray	Organizations are open to the idea of different tiers for adherence to safeguards. A majority are expecting NIST SP 800-171 requirements and timeline for the assessments. Questions arose regarding audit oversight: Self-assessments, regulations, program participation agreements (PPAs) and Student Aid Internet Gateway (SAIG) agreements. Senior leadership from OCIO, FSA, and OS attended.
ED Deputy Secretary meeting with external stakeholders and Senior Director, Governmental Auditing and Accounting, bringing together cybersecurity, state auditors, comptrollers and state treasurers to address Department financial management engagements with IHEs.		Completed	Jason Gray	The audit community has its own framework and the workforce would need to adapt adding cybersecurity auditing skills. A notice would need be necessary and have sufficient time to implement.
CIO Cyber Outreach Memo to improve information sharing and strengthen communications was posted.		Completed	Jason Gray	Memo supports Department outreach efforts to IHEs. https://er.educause.edu/blogs/2019/12/working-toward-a-new-information-security-relationship-with-the-us-department-of-education

Key Milestones

Milestone Summary				
Key Milestone	**Milestone Due Date**	**Milestone Status**	**Owner**	**Comments**
Issue guidance to IHEs to provide a definition of information security breach and when and how to report a breach	Q4 FY2020	In-Progress	Mia Jordan	While the Department has a definition of Breach OMB M-17-12, we are addressing community concerns as part of the IHE cyber taskforce directed by the FSA COO. Anticipate closing Q1 FY2021.
Establish secure mechanisms for breach notification, including secure storage for such information	Q4 FY 2020	In-Progress	Mia Jordan	The design work is underway and resource requirements are being identified.
Share best practices for building and maintaining secure and resilient systems.	Q4 FY2020	Completed	Jason Gray/Steven Hernandez	Briefed the Kentucky Society for Technology in Education (KYSTE) on March 12 regarding secure cloud and federal resources available to States.
FSA and SPPO, through PTAC, continued assisting IHEs	Q4 FY2020	Completed	Hermes Kevin/Mia Jordan	FSA and SPPO combined to deliver 56 outreach activities throughout FY 2020 exceeding the year end goal of 20.
Create a process through which IHEs can validate compliance notifications and reporting requests	Q2 FY2021	In-Progress	Mia Jordan	A manual process exists, based on email correspondence, but an automated method is being designed. The design requirements are being incorporated into the NextGen partner portal.
Develop cyber fraud article		TBD	Jason Gray/Steven Hernandez	On hold till post COVID.

Key Indicators

The Department will participate in 12 engagements with sector-related non-governmental organizations (NGOs).



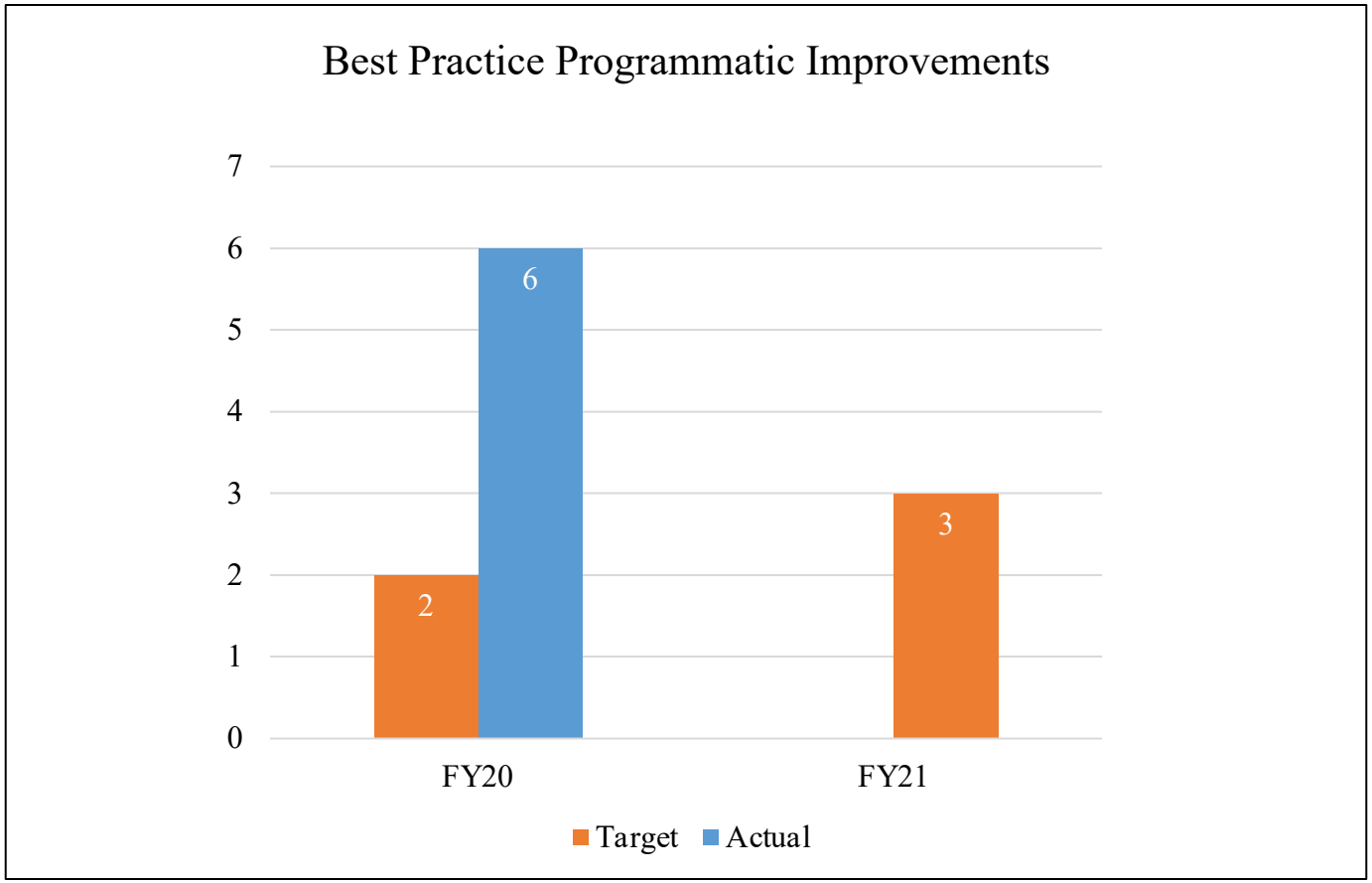
Key Indicators

The Department participated in 12 engagements with sector-related NGOs in FY 2020.

Actual NGO engagements in FY 2020	
NGO	**Description**
AASCU	American Association of State Colleges and Universities
AAU	Association of American Universities
APLU	Association of Public and Land- grant universities
EDUCAUSE	EDUCAUSE, Non-profit association (two engagements over Q2, Q3, and Q4)
FAME	FAME, commercial service provider in the IHE administrative space
KySTE	Kentucky Society for Technology in Education
NACUA	National Association of College and University Attorney
NACUBO	National Association of College and University Business Officers
NAICU	National Association of Independent Colleges and Universities
NASFAA	National Association of Student Financial Aid Administrators
NCHER	National Council of Higher Education Resources
PPHEA	Panhandle-Plains Higher Education Authority

Key Indicators

The Department will issue five best practice programmatic improvements.



Key Indicators

The Department issued six best practice programmatic improvements in FY 2020.

Actual Programmatic Improvements in FY 2020	
1	OCIO increased outreach through the CIO Cyber Outreach Memo written to the EDUCAUSE.
2	FSA issued a Technology Security Alert informing IHEs of issues and threats associated with Ransomware.
3	Department's Student Privacy Policy Office (SPPO) conducted four outreach technical assistance (TA) activities in Q2 FY2020 to institutions of higher education (IHEs)
4	IFAP.ed.gov Gramm-Leach-Bliley Act (GLBA) notice regarding Federal Trade Commission (FTC)
5	Collaborated with IHE's to provide technical assistance to assist with remediation and improve the cybersecurity posture during COVID-19.
6	The Department held targeted technical discussions and conference calls with four schools to discuss specific threat intelligence information discovered during FSA proactive research efforts.

Data Accuracy and Reliability

The Department continues its outreach and collaboration efforts with NGOs and its federal partners to protect the educational journey of students.

Department activities/efforts will be posted on a SharePoint site.

Additional Information

Contributing Programs

Organizations

- IHEs
- FSA
- OCIO
- OPEPD

Program Activities

- Enhanced outreach to IHEs
- Audits of GLBA-related information security safeguards at IHEs

Statutes/Authorities

- The Compliance Supplement identifies existing federal compliance requirements to be considered as part of an audit required by the Single Audit Act Amendments of 1996.
- The Compliance Supplement was updated, effective July 2019, to include requirements under the Gramm-Leach-Bliley Act (GLBA) Safeguards Audits to 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.

Additional Information

Stakeholder/Congressional Consultations

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.

The Department also conducted congressional consultation as part of the development of the *U.S. Department of Education's Strategic Plan for Fiscal Years 2018-22,* the FY 2018-2019 APGs, and the FY 2020-2021 APGs.