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: Kala Shah Surprenant, Acting Director of the Student Privacy Policy Office (SPPO), Office of Planning, Evaluation and Policy Development (OPEPD)

Performance.gov

Fiscal Year 2020, Quarter 1 & 2

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 Q1

- In Quarter 1, the Office of the Chief Information Officer (OCIO) increased outreach by having the Department's Chief Information Officer (CIO) write the CIO Cyber Outreach Memo to the EDUCAUSE community. The memo discusses the shared interests and concerns of the Department and higher education information technology leaders, professionals, and their institutions in the security of student aid data.
- The Department collaborated with EDUCAUSE to work on strengthening the common understanding of IHE protections for participants in Title IV programs. The engagements have produced a series of outcomes and common objectives for the Department and EDUCAUSE in areas such as a uniform definition for the term "breach," security compliance frameworks, and how the Department will engage Title IV program participants in the future.

Below is a summary of Quarter 1 engagements:

- The Department held Cybersecurity Stakeholder Meetings with the following nongovernmental organizations (NGOs):
    - National Association of College and University Business Officers (NACUBO), National Association of Independent Colleges and Universities (NAICU), Association of American Universities (AAU), EDUCAUSE, National Association of College and University Attorneys (NACUA), National Association of Student Financial Aid Administrators (NASFAA), American Association of State Colleges and Universities (AASCU), and the Association of Public and Land-grant Universities (APLU).
    - These organizations in the education community share a common cybersecurity goal to protect students' educational journeys.

Summary of Progress – FY 2020 Q1

The Department also had the following engagements:

- A Department collaborative team (OCIO/FSA) worked to improve information sharing and strengthen communications with partners and customers. To do so, the team identified opportunities at three levels to contribute to cybersecurity in the education community:
    - Operational - The Department and its federal partners, including the Department of Homeland Security (DHS) and the Federal Bureau of Investigation, can be of enormous assistance to the education community.
    - Tactical - In the near term the Department has opportunities to share best practices for building and maintaining secure and resilient systems.
    - Strategic - As the Department's programs change, it needs to understand how those changes affect education institutions.
- FSA held five cybersecurity training sessions for IHE administrators during the December 2019 FSA Training Conference. Each session covered breach definition and reporting requirements.
- FSA updated business processes to provide IHEs with immediate feedback when they have submitted a breach report or request. The process provides for immediate confirmation of receipt of the report, periodic communications periods based on the criticality of the status of the case (i.e., daily, weekly, or monthly), and a final disposition communication.
- FSA initiated an internal project to design a long-term, high availability solution to provide IHEs the ability to securely submit notifications and documentation to meet the breach notification requirements. The first action was to increase the automated case management tool capacity, by 15%, to provide additional secure storage for all cybersecurity incident and breach case materials and artifacts.

Summary of Progress – FY 2020 Q1

FSA and SPPO Outreach Efforts

FSA and SPPO, through the Privacy Technical Assistance Center (PTAC), continued assisting IHEs. For example:

- Southeast Regional Datatel User's Group (SEDUG) meeting on 11/20-21/19 included seven sessions targeting IHEs and focused on data privacy, security, and data breach response.

Summary of Progress – FY 2020 Q2

- The Department conducted meetings with EDUCAUSE and other similar organizations in the education community to discuss a common cybersecurity goal to protect students' educational journeys.

- During Quarter 2, the Department held Cybersecurity Stakeholder Meetings with the following nongovernmental organizations:
  - Panhandle-Plains Higher Education Authority, National Council of Higher Education Resources, and Third-Party Servicers.

- The Department's Chief Information Security Officer (CISO) met with the Kentucky Society for Technology in Education to discuss federal resources available to assist state, local, and tribal governments in protecting their enterprises.

- The Department (Office of the Secretary, SPPO and FSA) met with the Federal Trade Commission to discuss requirements of GLBA and the National Archives and Records Administration (NARA) for the protection of controlled unclassified information in non-federal systems and organizations.

Summary of Progress – FY 2020 Q2

- The Department held outreach conference calls with three IHEs to work through the threat intelligence information from possible account compromises. This was a great opportunity for FSA's Postsecondary Institutions Team (PSI Team) to demonstrate its proactive commitment to help IHEs improve their overall security postures.

- Further, the PSI Team demonstrated the commitment to protecting student data by participating in Data Privacy Champion Day through StaySafeOnline.org. The PSI Team was able to showcase its commitment to the greater education community by sharing resources and industry best practices.

- The Department's Student Privacy Policy Office (SPPO) conducted four outreach technical assistance (TA) activities, in Quarter 2, to IHEs on data privacy and information security issues. In January, the SPPO acting director participated in meetings with IHEs on privacy and information security and shared, through SPPO's Privacy Technical Assistance Center, data breach response training scenarios. In March, the SPPO acting director conducted a presentation on "FERPA and Virtual Learning during COVID-19" at https://studentprivacy.ed.gov. In March, SPPO provided TA to the data governance council of the Southern Regional Education Board, which works with 16 member states.

Key Milestones

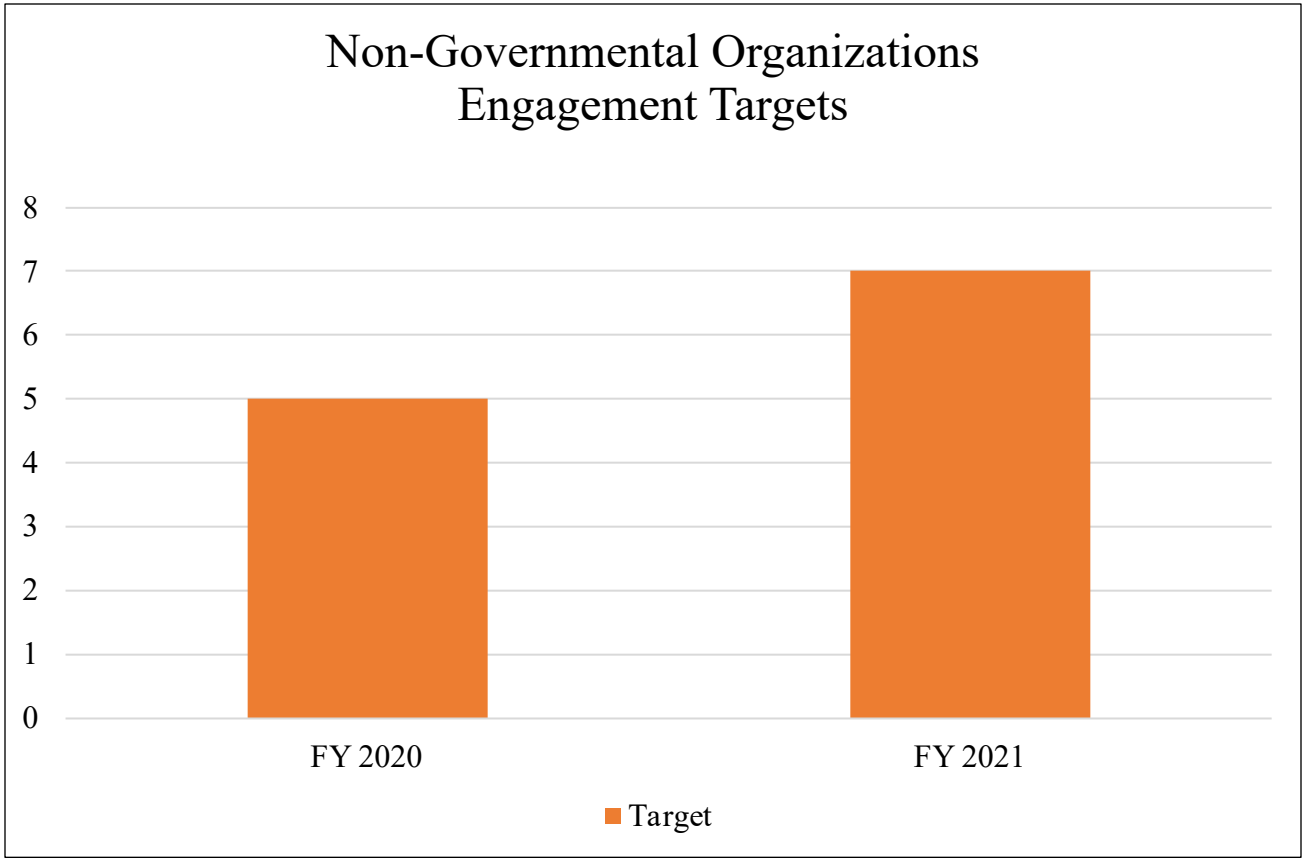
Milestone Summary					
Key Milestone	**Milestone Due Date** *[e.g., Q2, FY 2017]*	**Milestone Status** *[e.g., Complete, On-Track, Missed]*	**Change from last quarter** *[optional column]*	**Owner** *[optional column]*	**Comments** *[Provide discussion of Progress, changes from last update, Anticipated Barriers or other Issues Related to Milestone Completion]*
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** *[e.g., Q2, FY 2017]*	**Milestone Status** *[e.g., Complete, On-Track, Missed]*	**Change from last quarter** *[optional column]*	**Owner** *[optional column]*	**Comments** *[Provide discussion of Progress, changes from last update, Anticipated Barriers or other Issues Related to Milestone Completion]*
Issue guidance to IHEs to provide a definition of information security breach and when and how to report a breach	Q4 FY2020	In-Progress		Wanda Broadus	The definitions are in review with the Department and discussions are underway to determine the proper document or communication means to inform the IHE community.
Establish secure mechanisms for breach notification, including secure storage for such information	Q4 FY 2020	In-Progress		Wanda Broadus	The design work is underway and resource requirements are being identified.
Create a process through which IHEs can validate compliance notifications and reporting requests	Q2 FY2021	In-Progress		Wanda Broadus	A manual process exists, based on email correspondence, but an automated method is being designed.
Share best practices for building and maintaining secure and resilient systems.	Q4 FY2020	In-Progress		Jason Gray/Steven Hernandez	Briefed the Kentucky Society for Technology in Education (KYSTE) regarding secure cloud and federal resources available to States.
FSA and SPPO, through PTAC, continued assisting IHEs	Q4 FY2020	In-Progress		Kala Surprenant/ Wanda Broadus	
Develop cyber fraud article		TBD		Jason Gray/Steven Hernandez	On hold till post COVID

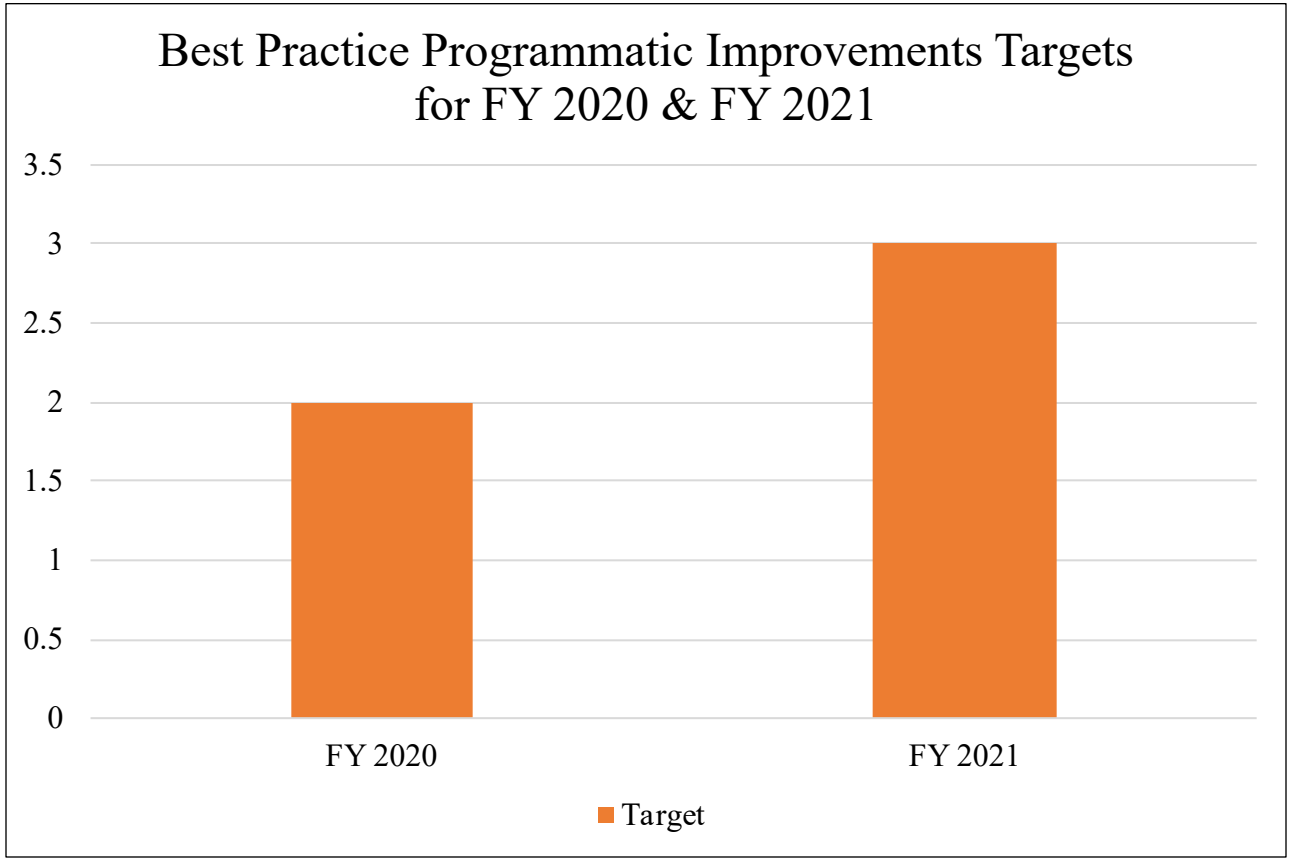
Key Indicators

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



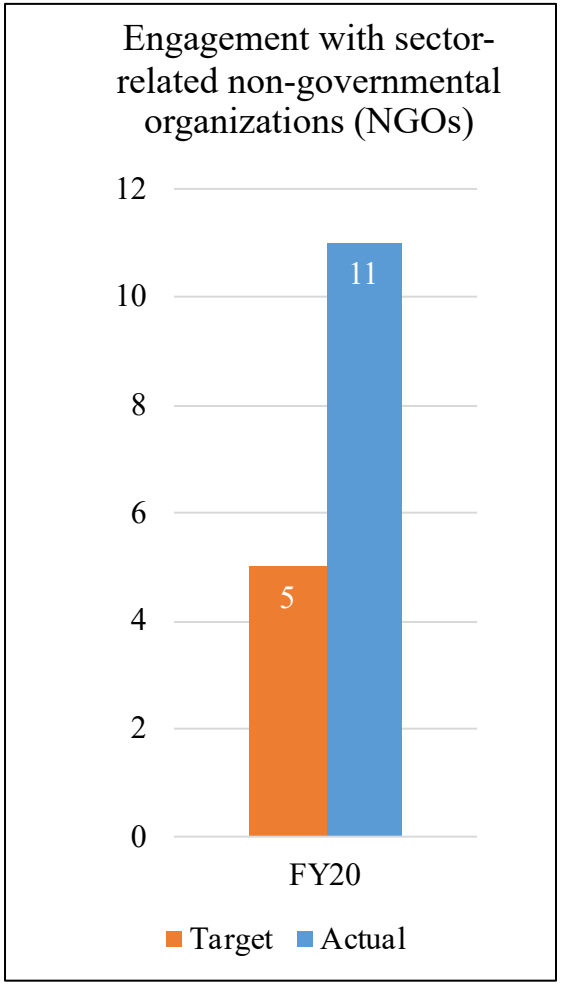
Key Indicators

The Department will issue five best practice programmatic improvements.



Key Indicators

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

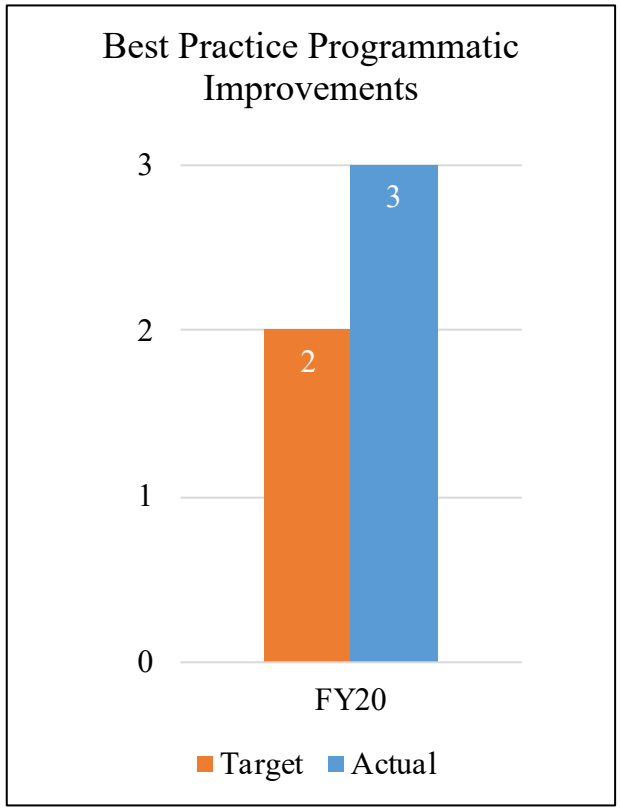


Actual NGO engagements in FY20

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
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.



Actual Programmatic Improvements in FY20	
1	OCIO increased outreach through the CIO Cyber Outreach Memo written to the EDUCAUSE
2	FSA team updated business processes to provide IHE's with immediate feedback when a breach report is submitted
3	Department's Student Privacy Policy Office (SPPO) conducted four outreach technical assistance (TA) activities in Q2 FY2020 to institutions of higher education (IHEs)

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.