EDUCAUSE Comments on
Federal Student Aid (FSA) Strategic Plan, 2020-24 (Draft)
October 21, 2020

Please note that EDUCAUSE attempted to submit these comments in full on October 21, 2020, via the comment form supplied by FSA for that purpose:

https://forms.office.com/Pages/ResponsePage.aspx?id=FEVdvd6EKEmp_WrhC7rWd13Tg73xs
r5FswsKKzzWb9ZUREZDTIFXTIU1V1o4Tkw0SFAwWEFPSUjYNy4u

Unfortunately, the comment fields for Parts 1 and 2 had character limits that would not accommodate our complete feedback on those parts of the plan. As a result, EDUCAUSE submitted this full set of comments to FSA on October 21, 2020, via email from Jarret Cummings, Senior Advisor for Policy and Government Relations, EDUCAUSE (jcummings@educause.edu), to FSAStrategicPlan@ed.gov.

Part 1: Trends in the Federal Student Aid Environment

Please specify the section of the draft Strategic Plan to comment on:

Trend 4: Increased Volume of Student Data Has Created New Opportunities, Obligations, and Risks.

Please specify the corresponding page number(s) in the draft Strategic Plan that relate to your comment(s):

pp. 29-30, 38

Please specifically describe your comments:

EDUCAUSE appreciates the comments made toward the end of page 30 regarding FSA’s desire to work with higher education institutions to advance our shared interest in information security related to student financial aid data. As EDUCAUSE, its members, and its fellow higher education associations have repeatedly stressed in public comments and direct dialogue with FSA, colleges and universities take very seriously the security and privacy obligations we share with FSA for the personal financial information entrusted to us both by students and their families. We have also repeatedly emphasized that effective, sustained partnership and collaboration between higher education IT leaders and professionals, other institutional stakeholders, and FSA offers the most productive path toward fulfilling those obligations. EDUCAUSE believes that the Department of Education and FSA have made great strides over the last few years in working with our community to better understand information security in
higher education, and we remain hopeful that the partnership and collaboration we have sought will come to fruition.

We are therefore disappointed with the tenor and content of this section, which seems intended to deflect information security concerns for student financial aid data onto colleges and universities as “the problem.” Vague references to the Department of Education and FSA rating highly on information security while “the education sector” rates poorly (p. 29) obscure a range of distinctions between educational institutions and their product and service providers; higher education and elementary and secondary education; traditional colleges and universities and for-profit higher education; and degree-granting institutions and postsecondary workforce training institutions. The closing text of this section itself acknowledges that organizational differences may make a substantial difference in organizational capacity to achieve the level of information security all stakeholders in student financial aid desire. Thus, EDUCAUSE urges FSA to revisit the text of this section to ensure that it presents a much more appropriately nuanced--and accurate--picture of higher education information security.

For example, the text introduces a problem that is carried throughout other relevant parts of the plan, and that frankly reflects a problem we highlighted for the Department of Education and FSA in comments we submitted to FSA in February 2018—the tendency to conflate actual breaches of personal information with general information security “events,” and the use of that conflation to imply institutional failures in relation to FSA data. First, the text cites the increase in institutional reporting of alleged breaches to FSA between 2015 and 2019 as indicative of a rising problem without supplying vitally important context. As we noted in our 2018 letter (https://library.educause.edu/resources/2018/2/educause-comments-fsa-breach-notification-information-security-reporting-requirements), the Student Aid Internet Gateway (SAIG) agreement provision that forms FSA’s breach requirement clearly indicates that the breaches in question relate to potential internal matters where “unauthorized personnel” at the institution have accessed relevant data. Given that such breaches occur on a relatively limited basis, it should be no surprise that the reporting number for 2015 is low, since it wasn’t until 2015 that FSA began to highlight the provision and attempt to apply a much more expansive interpretation of it. As we called out in our letter, this more expansive interpretation rests on the dubious conflation of “data breaches” with “security incidents” in general. In turn, this problematic conflation rests on the lack of clear definitions of either term in the context of the SAIG agreement as well as a lack of associated, publicly available guidance and a revamped reporting provision that appropriately distinguishes between them to establish clear, reasonable reporting expectations.

The citation to an EDUCAUSE report discussing higher education breach statistics further emphasizes our point about the misleading nature of this section’s implications. First, not only does the report itself pre-date the period in which FSA began revisiting the SAIG agreement breach reporting provision in a new and more expansive way (again without revising the text of the provision to reflect that interpretation or providing guidance or process to inform compliance), it covers data from 2005-2013, making it clearly even more outdated as a basis of comparison for the current period than the report’s 2014 publication date would already indicate.
For example, during the period covered by the report, the number of state data breach notification laws increased significantly, and existing laws changed substantially as well. We also know that notification laws have continued to evolve and proliferate through the current timeframe. Thus, even at the time of publication, the trend line for notification volume had to be seen through the lens of other factors that could account for year-to-year changes in the number of notifications. Extrapolating from that rough analysis to the current period and attempting to frame it as somehow definitive in explaining any present issues would therefore require, at a minimum, significant additional statistical work that the text of the plan does not address.

Furthermore, the text of this section overlooks important parts of the report it cites. Of the 727 education sector breaches identified, only 551 were attributed to colleges and universities, with “the data hint[ing] at a downward trend in the number of breaches reported over time...” (Just in Time Research, p.3) Likewise, this section does not include the key findings from the report’s analysis, which sets the statistics in the proper context:

*Education, and particularly higher education, is often singled out as having a large number of reported data breaches, and at first look, the PRC database appears to confirm that view. Look more closely at the data, however, and a different picture emerges. As an industry, education has some of the lowest counts of records exposed per breach incident—the number of reported breaches in the education industry does not mean more records containing personally identifiable information are being compromised.*

*Many speculate that higher education’s culture of openness and transparency encourages breach reporting by institutions, even when such reporting is not legally necessary. This culture does not exist in other industry sectors, where breach reporting could damage an organization’s ability to be competitive in that industry. In these instances, a breach may only be reported when it is required by a law or some other regulation, and even then, only when the breach circumstances clearly fall within the purview of the underlying regulation.*

*Higher education as a unique sector has long engaged in cooperative activities designed to improve the information security posture of all institutions...* (Just in Time Research, p.6)

Finally, and perhaps most importantly in evaluating the relevance of the EDUCAUSE report for the points that this section is trying to make, the report says nothing about whether the 551 higher education breaches that occurred over the course of almost a decade and almost a decade ago had anything to do with FSA data. Since the SAIG agreement is intended to cover FSA data exchanged with institutions via the SAIG, reading the breach provision in context would clearly lead one to construe that only breaches involving FSA data would have been relevant to the breach reporting provision, with the provision’s reference to access by unauthorized personnel further restricting the scope of breaches relevant for reporting purposes. Thus, the section’s point that “only two percent” of these breaches had been reported to FSA...
overlooks the very real possibility that only two percent of the breaches in question should have been reported to FSA given the data and the breach reporting provision involved.

Rather than stretching the statistics cited beyond their meaningful context, this section would better serve both FSA and the higher education community if it instead focused on the general information security environment and drew reasonable inferences from it to the higher education context. We can all agree that maintaining the security and privacy of student financial aid data is a constant challenge, with a threat environment that is continuously evolving, and that no matter what institutions and FSA do separately and collectively to bolster that security, there will always be more for us to do, separately and collectively. Implying a lack of commitment by institutions to information security as well as their FSA compliance obligations serves no one well. EDUCAUSE would encourage FSA to reframe this section to instead discuss the necessity of FSA and Department of Education engagement with relevant higher education stakeholders concerning the establishment of shared frameworks and guidance for key information security issues related to FSA data.

We would carry our points on the statistic regarding the increase in “cybersecurity event” reporting between 2015 and 2019 over to the strategic goal milestone discussed on page 38 of the plan as well. To that, we would add our concern that questions EDUCAUSE has previously raised about the IHE Cyber Team have remained unanswered. The nature of the team, its reporting lines and authority, plans for engagement with the higher education information security community, and the ways in which open lines of communication and collaboration with the community will be established all remain unknown to our members. This seems highly problematic given that this unit is ostensibly intended to serve the objective of increasing cybersecurity assistance to higher education institutions.

**Part 2: Strategic Goals and Objectives**

Please specify the section of the draft Strategic Plan to comment on:

Strategic Goal 4: Strengthen Data Protection and Cybersecurity Safeguards.

Please specify the corresponding page number(s) in the draft Strategic Plan that relate to your comment(s):

pp. 54-56

Please specifically describe your comments:

Regarding Strategic Objective 4.2, “Improve student privacy data and cybersecurity controls of IHEs through outreach and communication, to mitigate future cyber incidents and breaches,” which is discussed on pages 54 and 55, EDUCAUSE appreciates FSA’s stated interest in collaborating with institutions and other stakeholders “inclusive of sharing best practices and
threat information” (p. 55). EDUCAUSE members and staff have consistently raised with FSA and the Department of Education the need for a well-defined process through which FSA and the department can work with our member chief information officers (CIOs), chief information security officers (CISOs), chief privacy officers (CPOs), and other higher education IT/information security leaders and professionals to extend the benefits of the effective practices and threat information sharing work in which EDUCAUSE members already engage for the benefit of the broader Title IV community. We hope the reference to those concepts here indicates that discussions on how best to accomplish them will soon begin in earnest.

That said, we take issue with the implication of this section that higher education institutions are subject to any greater incidence of attempted information security compromises than any other major sector, or that the response of our member institutions to such attempted compromises is less strenuous or effective than that of other, similarly situated organizations. The first paragraph under the subheading for Strategic Objective 4.2 asks the term “significant evidence” to do a great deal of work when it only “suggests” an increasing volume of incidents that “potentially” might indicate increasing risk for FSA data and systems, as well as students and families by extension. Again, context matters—attempted compromises are rising across all sectors of our society and economy; all organizations have to take risk-based approaches to addressing this volume and mitigating potential negative outcomes; and neither this section nor the plan as a whole identifies evidence that colleges and universities are any less effective in their risk management or mitigation efforts. To suggest otherwise is deeply unfair and unnecessarily complicates the dialogue that FSA, the department, and the EDUCAUSE community have begun on working toward greater collaboration and information sharing.

Also, we see in this section once again the conflation of information security incidents with breaches and the assertion that institutions should “report cyber incidents when they occur.” As noted in our 2018 comments as well as subsequent communications, FSA has yet to define effectively its basis of authority for potentially requiring “incident reporting” as compared to “breach reporting.” Per those comments, even if clear authority for “incident reporting” could be identified, appropriately defining and publicly documenting the scope and requirements for such reporting would be critical to avoid FSA being flooded on a minute-by-minute basis with every phishing email or questionable URL that comes to any institution’s attention. Furthermore, while the SAIG agreement includes a breach reporting provision, we discuss elsewhere in our comments on this strategic plan as well as in prior writings to FSA and the department, how the lack of content in the provision as well as a lack of accompanying documentation and procedures creates, at best, an ad hoc environment for compliance.

Finally, to the extent that the Department of Education and/or FSA might seek to “utilize existing and future legislation” to further information security objectives, EDUCAUSE believes that such steps should be taken only after the higher education IT/information security community and other stakeholder communities have had the opportunity to provide substantial input on the proposed measures. The likelihood of any such steps achieving success, either legislatively or subsequently, would be much greater if they are informed by the knowledge and experience of higher education leaders and professionals and have broad stakeholder support.
Pages 55-56 discuss the metrics that FSA will use to assess progress toward achieving Strategic Goal 4. We would ask FSA to please note again the conflation of incidents with breaches and ask you to consider our previous comments about that problem. In terms of the metrics themselves, EDUCAUSE would argue that focusing on “the number of institutions identified with cybersecurity findings based on annual OMB compliance audits” and measuring “the increase in IHE cybersecurity effectiveness by reducing GLBA cybersecurity non-compliance” (p. 56) is likely to be problematic for the near-term. As EDUCAUSE, the National Association of College and University Business Officers (NACUBO), and other higher education and auditing organizations raised with FSA and OMB during and following the development of the Federal Trade Commission (FTC) Safeguards Rule audit objective, the institutional and auditor communities currently lack a framework, much less a shared framework, for establishing institutional compliance with the elements of the Safeguards Rule that the audit objective covers. With the audit objective having just come into effect with the FY19 audit process, it will likely take at least a couple more fiscal years before clarity is achieved among all parties on what institutions need to document and how to confirm compliance with the objective. Until that occurs, institutions and FSA will likely see a number of “false positives” that institutions can readily resolve once the nature of the disconnect is identified. If FSA makes determinations on Safeguards Rule compliance based on these early results, it could easily lead to suboptimal approaches and outcomes for all concerned.

EDUCAUSE also notes the discussion of FSA’s intent to “develop and execute a threat reduction program” as part of its effort to help institutions through “sharing threat information” (p. 56). We again appreciate FSA’s interest in working with the higher education community on expanding collaboration around threat information sharing. We likewise, though, stress that effectiveness in this area depends on establishing a strong partnership between FSA and the institutional community, and between FSA and higher education information security leaders and professionals in particular. EDUCAUSE looks forward to working with FSA and the department to facilitate the process of engagement with our members that such an effort requires.

**Part 3: Performance Measures for Strategic Goals**

Please specify the section of the draft Strategic Plan to comment on:

Performance Measures for Goal 4

Please specify the corresponding page number(s) in the draft Strategic Plan that relate to your comment(s):

pp. 68
Please specifically describe your comments:

The plan proposes to use FY20 as the baseline from which to calculate improvement in the reduction of Safeguards Rule audit findings. Since the audit objective was just implemented for the first time with the FY19 federal single audit process, however, setting the baseline starting with FY20 seem likely to give an inaccurate view of institutional compliance as discussed in the EDUCAUSE comments on Strategic Goal 4. In commenting on the then-proposed implementation of the Safeguards Rule audit objective for the FY19 audit process, the audit community stated that it did not yet have a common framework from which auditors and institutions could work to address the objective, leaving each institution and its external auditors to negotiate individually what institutional documentation would establish compliance. FSA itself has likely already seen a number of “false positives” arise from this situation, with institutions ultimately able to prove their compliance to FSA’s satisfaction once clarity about what institutional documentation is relevant in a given case has been achieved. With this in mind, EDUCAUSE recommends that FSA consider setting the baseline year for Part A of the Strategic Objective 4.2 performance metric at least at FY21. That is much more likely to give institutions and their auditors the time they need to consult with each other and FSA to ensure that the basis for institutional compliance with the Safeguards Rule audit objective has been fairly and clearly established.

Regarding Part B of the performance metric for Strategic Objective 4.2, EDUCAUSE also recommends that FSA shift the baseline year for measurement from the proposed FY21 to at least FY22. As previously discussed, EDUCAUSE and its members remain deeply concerned about the apparent conflation of “data breaches” with “cybersecurity incidents” in FSA’s thinking as reflected in this strategic plan. Establishing a shared understanding between FSA and the higher education IT/information security community regarding what constitutes a “cybersecurity incident” as compared to a “data breach,” as well as what the appropriate authorities, processes, and procedures are for addressing one or the other, remains a paramount consideration for effective collaboration and reasonable compliance expectations. That those issues remain largely unaddressed even as FSA, the department, and EDUCAUSE have maintained ongoing conversations indicates that a comprehensive process to resolve them will be necessary. The planning and outreach required for such a process means that one likely couldn’t start until well into 2021, and the need to ensure general awareness of the outcomes to allow for broad-based reporting likely means that FY22 is the earliest that institutional reporting might reasonably be measured to set a performance baseline.