PERSPECTIVES

US Federal Policy

Jarret Cummings, with the EDUCAUSE Policy Advisory Committee (EPAC)

The EDUCAUSE Policy Advisory Committee (EPAC) provides community members’ insights into federal policy issues that impact information technology in higher education. Committee members span a variety of senior leadership roles and help the EDUCAUSE Policy Team identify, understand, and respond to legislative or regulatory developments that could have significant implications for our community. With this mission in mind, the EPAC dedicated its last formal meeting of 2019 to exploring where current federal policy issues connect with the EDUCAUSE 2020 Top 10 IT Issues.

Not surprisingly, concerns about information security and data privacy at a national level dovetailed with the top two issues for 2020: Information Security Strategy (#1) and Privacy (#2). The committee reflected on the substantial time that EDUCAUSE members and staff spent this year evaluating the sweeping changes to the Safeguards Rule proposed by the Federal Trade Commission (FTC) as well as efforts by the National Institute of Standards and Technology (NIST) to introduce “controlled unclassified information” (CUI) guidelines specifically for federally funded research projects designated as “critical programs” or “high value assets.” In light of these and related developments, the committee stressed the importance of understanding legal and audit compliance in order to effectively manage security and privacy. EPAC members expressed particular concern about the growing tendency of legislative and regulatory proposals in these areas to emphasize prescriptive “checklists” of requirements, as opposed to supporting compliance based on risk management, which is widely recognized as effective practice. The committee agreed that EDUCAUSE should continue to actively work with its higher education association partners to press for a focus on prioritizing and managing risk as the key to preserving information security and data privacy.

Turning more specifically to the issue of CUI requirements as a particular subset of security and privacy challenges in higher education, EPAC members noted how US Department of Defense (DOD) developments may presage a wider federal trend toward more direct mandates. While compliance with the NIST Special Publication (SP) 800-171 CUI standards has been incorporated into DOD grants and contracts for almost two years, the department’s dissatisfaction with the progress of security assurance among its contractors has led it to propose a Cybersecurity Maturity Model Certification (CMMC) program. This program would incorporate the 800-171 requirements, along with a mix of other guidelines and standards, to define the level of information security that a given organization has achieved, with certification based on external auditing.

While the impact that the CMMC process may have on affected colleges and universities is not yet clear, EPAC members believe that an audit-based certification program would have the unfortunate effect of reinforcing a requirement “checklist” mindset. To illustrate this problem, a committee member cited a DOD effort to incorporate CUI requirements into an institutional contract regardless of whether the project actually involved CUI. Such a move would create unnecessary compliance costs that an industry-standard, risk-based approach might largely avoid. Likewise, the originator of federal CUI guidelines, NIST, may itself serve as an example of the mechanical application of “checklist” requirements, despite the references in its various publications to the importance of risk-based approaches. The EPAC discussed the example of an institution that faces a NIST-proposed contract that would require the institution to adopt NIST SP 800-53 federal agency information security guidelines, which are much more stringent than the 800-171 standards, even though the project has no major security implications.

On the plus side, the committee noted that the proposed “critical program / high value asset” CUI guidelines (NIST SP 800-171B) remain on hold, pending the resolution of Office of Management and Budget (OMB) reviews of related regulations. Committee members expressed hope that this will give NIST and DOD, which worked with NIST on the proposal, time to fully consider the problems with the draft guidelines that the higher education community raised. In particular, higher education groups asked NIST and DOD to resolve the major ambiguity regarding the timing and basis for designating a grant or contract as involving a “critical program” or “high value asset,” including how other agencies might apply those guidelines in ways that NIST and DOD may not have anticipated.

The committee discussed the extent to which the general federal CUI guidelines (NIST SP 800-171) have already influenced agencies’ compliance expectations. For example, while the implementation of the guidelines on the non-defense side of the federal government continues to be delayed, committee members cited US
Department of Education (ED) guidance (dating from 2015 and 2016) that strongly encourages institutions to follow 800-171. With that in mind, and given the existing application of 800-171 to DOD contracts, EPAC members agreed that institutions should be incorporating the 171 guidelines into their security programs in anticipation of an eventual ED mandate.

Committee members also explored the link between the impact of federal policy on the top two 2020 IT Issues and its implications for Higher Education Affordability (#8) and Administrative Simplification (#9). For example, the committee as a whole worried about the increased complexity and costs associated with the mandates-based “checklist” approach to security and privacy and what those rising costs could mean for institutional budgets and, ultimately, tuition rates. From the committee’s perspective, the potential for increased institutional burdens to become increased financial burdens for students further reinforces the necessity for federal agencies to recognize risk management as the basis for effective security and privacy management.

Looking at these issues in the context of academic research, EPAC members argued that agencies should allow institutions to charge the expenses for security and privacy mandates related to a federal grant or contract as a direct cost to the project. In addition, the committee suggested that funding agencies should add a direct percentage to institutions’ indirect cost rates to account for the impact of sponsored research security and privacy requirements on overall technical and compliance environments. The EPAC expressed concern that costs for research security may already be outstripping the resource capacity of many institutions and that the situation will only get worse without changes like those suggested. Members acknowledged that the committee’s proposals would reduce the grant or contract funds available for the sponsored activity. Nevertheless, they consider these proposals—or other means of increasing resources for security and privacy—as essential for keeping institutions from cutting corners on compliance or from sacrificing research opportunities.

The discussion of security issues related to academic research gave way to a conversation about balancing the implications of institutions’ broader engagement with the world. The committee agreed that advancing academic programs and research increasingly entails international collaboration and cooperation, with people, knowledge, and data moving freely across campus and national borders. This, unfortunately, can also expose institutions to nation-state efforts to exploit such openness for illicit gain and influence. Reconciling the need to appropriately secure institutional communities while sustaining the openness and international connections on which they often thrive remains a challenge uniquely relevant to higher education, and the committee noted that this challenge has financial impacts as well. Committee members indicated, for example, that immigration and national security concerns appear to be driving steep reductions in foreign student enrollment, particularly from China. As evidence, a member cited the case of an institution that has already lost $30 million in tuition revenue due to declining foreign student enrollment, leading to program cuts and layoffs.
Reflecting on these concerns, the committee coalesced around the need for strengthening a “whole institution” perspective that would facilitate *Administrative Simplification* (#9) and contribute to resource efficiencies and, ultimately, college affordability. The committee noted that such an approach could also benefit internal systems and processes, which often remain unnecessarily complex and therefore costly. Campus compliance offices, with their existing institutional perspectives, would be natural partners in this holistic approach.

The committee also discussed how the intersection of *Higher Education Affordability* (#8) and *Student Retention and Completion* (#6) presents a major challenge for all but the most well-resourced institutions. Members noted the extent to which students at many institutions have little financial cushion for even small, unexpected expenses. The committee indicated that these problems are manifested in the growing rates of food and housing insecurity among their student bodies. For example, at one committee member’s institution, well over 15 percent of students are food-insecure. EPAC members talked about institutional efforts to respond, including the creation of special funds carved from institutional budgets and endowments to provide small emergency loans as well as food and housing assistance.

The potential for institutions to enhance student success by taking a more holistic view of student services and support (*Student-Centric Higher Education*, #5) was also discussed. One EPAC member noted, for example, that facilitating more stable access to food and housing could be just as impactful in helping students succeed as “nudges” from learning analytics programs. Another committee member cautioned, though, that the scope and complexity of a “whole institution” approach may vary widely based on the relevant aspect of the institutional mission or goal and noted that working to address compliance risk on an institution-wide basis involves factors and processes that are much more within the institution’s control, as compared with trying to help students cope with socioeconomic factors that extend far beyond campus.

The committee closed its review of where federal policy and the 2020 Top 10 IT Issues intersect by discussing the corrosive effect of public skepticism regarding the value of higher education on achieving *Sustainable Funding* (#3) for the institution and its IT needs. While research continues to show that the value of higher education to students’ economic prospects has never been higher, negative anecdotes about individual cases of excessive debt and lack of career progress have created and sustain a national narrative about how colleges and universities lack a commitment to student achievement. The resulting skepticism impacts the willingness of the public to fund higher education. This only heightens the need for the EDUCAUSE community to meet the challenges presented by the 2020 Top 10 IT Issues, all of which either directly or indirectly influence the capacity of colleges and universities to foster student success.

“While research continues to show that the value of higher education to students’ economic prospects has never been higher, negative anecdotes about individual cases of excessive debt and lack of career progress have created and sustain a national narrative about how colleges and universities lack a commitment to student achievement.”

— Jarret Cummings, Senior Advisor for Policy and Government Relations, EDUCAUSE

© 2020 Jarret Cummings and the EDUCAUSE Policy Advisory Committee (EPAC). The text of this work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Jarret Cummings (jcummings@educause.edu) is Senior Advisor for Policy and Government Relations at EDUCAUSE.