March 29, 2017

Gilbert Tran
Office of Federal Financial Management
U.S. Office of Management and Budget
New Executive Office Building, Room 6025
Washington, DC 20503

Dear Mr. Tran:

On behalf of the National Association of College and University Business Officers (NACUBO), EDUCAUSE, the Council on Governmental Relations (COGR), and the National Association of Student Financial Aid Administrators (NASFAA), we write to express our concerns with the U.S. Department of Education's (ED) proposed audit objective as stated in Student Financial Assistance (SFA) Cluster Special Tests and Provisions §14, *Securing Student Information*, contained in the 2017 Compliance Supplement Vett Draft. Primarily, we are concerned that the proposed audit objective is overly broad in scope and lacking in specificity, and thus will lead to a compliance regime that is more arbitrary and capricious than consistent and beneficial. As written, §14 would escalate audit work that is currently unplanned and unbudgeted—increasing cost and burden for higher education institutions. As such, our associations request that the Office of Management and Budget (OMB) work with our community to revise the approach to implementing §14 in a manner that will address the concerns we raise in this letter.

NACUBO represents more than 2,100 colleges, universities, and higher education providers. It represents chief business and financial officers through advocacy efforts and professional development activities. NACUBO's mission is to advance the economic viability and business practices of higher education institutions, including in the information technology (IT) space, to support the fulfillment of their academic missions.

EDUCAUSE is a nonprofit association and the foremost community of information technology leaders and professionals committed to advancing higher education. Its membership includes approximately 2,000 colleges and universities, 350 corporations serving higher education IT, and dozens of other associations, state and federal agencies, college and university system offices, and not-for-profit organizations. EDUCAUSE strives to support IT professionals and the further advancement of IT in higher education through analysis, advocacy, community- and network-building, professional development, and knowledge creation.

COGR is an association of 190 leading universities and research institutions. Member institutions conduct over $60 billion annually in research and development activities and play a major role in performing basic research on behalf of the federal government. COGR brings a unique perspective to regulatory and cost burden and focuses on the influence of federal regulations, policies, and practices on the performance of research and other sponsored activities carried out at COGR member institutions.

NASFAA represents more than 20,000 financial aid professionals at nearly 3,000 colleges, universities, and career schools across the country. All told, NASFAA members serve nine out of every ten undergraduates. NASFAA provides professional development for financial aid administrators; advocates for public policies that increase student access and success; serves as a forum on student financial aid issues, and is committed to diversity throughout all activities.

NACUBO, EDUCAUSE, COGR, and NASFAA thoroughly support securing the privacy and confidentiality of student information through the use of robust, mindfully constructed, and well-executed information security plans. Institutions of higher education have continuously ensured that such plans are in place through their compliance with the Safeguards Rule established pursuant to the Gramm-Leach-Bliley Act (GLBA) over the fourteen years since the Rule took effect.

Given the many years since the Rule's enactment and the ongoing cybersecurity concerns that a continuously evolving IT environment brings, our groups have regularly reached out to regulators to open discussions about the status and progress of higher education information security – both separately and as part of the broader higher education community. For example:

- NACUBO, EDUCAUSE, and NASFAA, along with other higher education leadership groups (including the American Council on Education) and IT experts, met with the undersecretary of education, Federal Student Aid (FSA) representatives, and other ED officials in December 2015 to discuss broad, consistent engagement on shared information security concerns.

- In September 2016, NACUBO and audit spokespersons met with OMB and ED representatives, including FSA staff, to evaluate items for inclusion in the 2017 Compliance Supplement. Although cybersecurity was a topic, auditors in attendance strongly advised ED to proceed with an incremental audit approach that included outreach and education about known concerns.

- In October 2016, EDUCAUSE met with FSA officials about possible changes to the FSA participation agreement and audit requirements related to information security.

Based on these contacts, our associations were very surprised to learn that an additional requirement as impactful as the proposed audit objective established in §14, *Securing Student Information*, would proceed toward implementation without any specific dialogue with our members or the higher education community in general.

Given this lack of prior engagement, we would draw OMB's attention to the comments of the National State Auditors Association (NSAA) dated February 17, 2017.[1] As NSAA writes, the audit objective included in §14 and its related provisions is both overly broad in scope and lacking in specificity in such a way as to be both difficult for auditors to assess and even more difficult for higher education institutions to comply with. We are also aware of the AICPA's

[1] http://nasact.membershipsoftware.org/files/Federal_Relations/Congressional_Reg_Comments/2017_02_17_Securing_Student_Information.pdf

strong objection to §14 and its recommendation to OMB that §14 be removed from the 2017 Supplement; based on our knowledge we support that recommendation.

Undoubtedly, institutions remain accountable for Safeguards Rule compliance. However, the Rule was purposely crafted with flexibility, allowing an organization to assess its risks and develop a security plan that fits its unique context based on the standard(s) that best applies to it. Higher education institutions are incredibly diverse, encompassing a wide variety of missions, operations, and student populations. They may hold roughly similar data related to student financial aid, but that data forms only part of the security environment they must manage.

Due to notable differences in institutional IT environments and associated security risks, as well as the amount of student information stored at each college or university, institutions rely on the flexibility of the Safeguards Rule to adopt information security plans that meet the actual needs of their campuses as opposed to an arbitrary standard. Colleges and universities focus on risk-based, integrated approaches to defining and deploying appropriate safeguards. This allows them to account for the full range of information they must secure and requirements they must meet. How each institution designs its information security program reflects the totality of its unique needs and related risk assessments, which includes the numerous federal and state information security standards it already faces. Because the particulars of these plans can, and should, vary between institutions, there is no way an institution can ensure it is adequately meeting the requirements of the proposed audit objective unless it is rewritten based on objective criteria. Without objective criteria, institutions and auditors will find themselves in a significantly more unpredictable audit process, where matters that the Safeguards Rule deliberately leaves to the discretion of the institution (e.g., not whether it conducts a risk assessment, but how it conducts its risk assessment) are likely to become subjects of debate and dispute. This could substantially undermine the audit process in terms of accurately assessing institutional compliance with the Safeguards Rule.

Additionally, the broad scope of the proposed audit objective would force auditors to specifically engage IT audit specialists to address the newly mandated, very expansive requirement. This extra expense would undoubtedly be passed on to colleges and universities. At this point in the fiscal year, most institutions have already budgeted for their anticipated FY17 audit costs; to unexpectedly face a much larger expense than expected would leave schools scrambling for extra funds. As nonprofit institutions, colleges and universities do not maintain large disposable cash reserves on hand; for most colleges and universities, a large unexpected charge means redirecting funds that were otherwise intended to support their educational, research, and public service missions.

Given the potential impact of the proposed audit objective, NACUBO, EDUCAUSE, COGR, and NASFAA recommend that OMB accept the NSAA and AICPA recommendations and either:

(1) Remove the new objective pending discussions with the higher education community to formulate a more appropriate, sustainable approach, or

(2) Rewrite the objective so that it contains objective criteria and delay its implementation until the FY18 single audit so institutions can plan for any additional audit expenses that may still result.

Further, we urge OMB and ED to increase collaboration and communication with the affected communities—including both auditors and representatives of institutions of higher education familiar with audit and cybersecurity processes. Without proper discussion and analysis, oversight becomes burdensome and inefficient, as we fear would be the case here, rather than effective at reducing and eliminating risk.

Respectfully,

Liz Clark
Director, Federal Affairs
NACUBO
lclark@nacubo.org

David Kennedy
Director, Costing Policies
COGR
DKennedy@COGR.edu

Jarret Cummings
Director, Policy and Government Relations
EDUCAUSE
jcummings@educause.edu

Megan McClean Coval
Vice President, Policy and Federal Relations
NASFAA
mccleanm@nasfaa.org

cc:

Mark A. Reger, U.S. Office of Management and Budget (Mark_A_Reger@omb.eop.gov)
Victoria W. Collin, U.S. Office of Management and Budget (Victoria_W._Collin@omb.eop.gov)