National State
Auditors Association
An Affiliate of NASACT

Headquarters Office
449 Lewis Hargett Circle, Suite 290
Lexington, KY 40503-3590
P (859) 276-1147, F (859) 278-0507
www.nasact.org

Washington Office
The Hall of the States
444 N. Capitol Street, NW, Suite 234
Washington, DC 20001
P (202) 624-5451, F (202) 624-5473

NSAA

February 17, 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:

Thank you for the opportunity to provide input on the 2017 Compliance Supplement Vett Draft. We have comments on various parts of the Compliance Supplement that have been sent to you separately. This letter and the accompanying attachment provide our input on the requirements proposed in the Department of Education's (ED's) Student Financial Assistance Cluster Special Tests and Provisions section, number 14 *Securing Student Information*.

We agree that it is very important for institutions of higher education (IHEs) to secure students' personal information and that IHEs should adopt reasonable safeguards to ensure confidentiality and protect the information against possible threats, fraud, and abuse. In addition, auditors who are responsible for auditing the student financial assistance cluster under the Single Audit Act should obtain an understanding of the access and security controls protecting student information associated with SFA awards.

However, the audit objective included in ED's 14th special test and provision over securing student information appears to be broader than, and go beyond, the audit procedures described. This makes it difficult for auditors to understand the specific compliance requirements for which they are required to provide an opinion over compliance, and the extent of test work that they should perform.

Because student information is stored and processed within systems, the core of ED's new audit objective deals with an IHE's ability to secure its information technologies. As stated earlier, we believe securing information technologies is important and already consider it in the evaluation of internal controls as part of a single audit. As a result, we took great time to review the new proposed audit objective to determine if:

- It is consistent with how other requirements for securing information systems are incorporated into the scope of a single audit;
- Its wording would allow for different auditors, given the same set of facts, to come to the same conclusion; and
- In substance, is it requiring auditors to provide more than an opinion on compliance.

Because of the importance of securing information technologies and the historical precedent that this new audit objective could have on future single audits, the attachment to this letter contains our comments on the new audit objective in special tests and provisions #14.

Overall, we believe OMB needs to reevaluate the new audit objective related to securing student information and either (1) remove the new audit objective in special tests and provisions #14 and take a measured approach to ensuring information technologies are secure, or (2) rewrite the new

National State
Auditors Association
An Affiliate of NASACT

audit objective so that it contains objective criteria. If OMB elects to leave the new audit objective as it is currently written, then OMB should notify the IHEs of the ramifications it will have on the scope of work and cost for the 2017 single audit and beyond.

Should you have any questions or wish to discuss further, please contact Kinney Poynter, NASACT's executive director, at (859) 276-1147, or me at (804) 225-3350.

Respectfully,

Martha Mavredes
Chair, NSAA Single Audit Committee
Auditor of Public Accounts, Virginia

Attachment

Student Financial Assistance (SFA) Programs
Special Tests and Provisions No. 14

Background

In the 2017 Compliance Supplement Vett Draft, OMB is proposing that the U.S. Department of Education (Education) require auditors to obtain sufficient appropriate audit evidence to support the following audit objectives (bolding and underlining added):

Audit Objectives – Determine whether the IHE has developed, implemented, and maintained a comprehensive information security program in accordance with the **Safeguards Rule**. *(Compliance Supplement Vett Draft 5-3-53, April 2017)*

Audit Objective – Obtain an understanding of internal control, assess risk, and test internal control as required by 2 CFR section 200.514(c). *(Compliance Supplement 3.2-N-1, June 2016)*

2 CFR section 200.514(c):

> (c) Internal control.
>
> > (1) The compliance supplement provides guidance on internal controls over Federal programs based upon the guidance in Standards for Internal Control in the Federal Government issued by the Comptroller General of the United States and the Internal Control—Integrated Framework, issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
> >
> > (2) In addition to the requirements of GAGAS, the auditor must perform procedures to obtain an understanding of internal control over Federal programs sufficient to plan the audit to support a low assessed level of control risk of noncompliance for major programs.
> >
> > (3) Except as provided in paragraph (c)(4) of this section, the auditor must:
> >
> > > (i) Plan the testing of internal control over compliance for major programs to support a low assessed level of control risk for the assertions relevant to the compliance requirements for each major program; and
> > > (ii) Perform testing of internal control as planned in paragraph (c)(3)(i) of this section.
> >
> > (4) When internal control over some or all of the compliance requirements for a major program are likely to be ineffective in preventing or detecting noncompliance, the planning and performing of testing described in paragraph (c)(3) of this section are not required for those compliance requirements. However, the auditor must report a significant deficiency or material weakness in accordance with §200.516 Audit findings, assess the related control risk at the maximum, and consider whether additional compliance tests are required because of ineffective internal control.

According to Education's section of the OMB Compliance Supplement, "[t]he **Safeguards Rule** requires financial institutions to:

a. Designate an employee or employees to coordinate the institution's information security program.

b. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of the institution's operations, including:

    (1) Employee training and management;
    (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
    (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

c. Design and implement information safeguards to control the risks the institution identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

d. Oversee service providers, by:

    (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
    (2) Requiring the institution's service providers by contract to implement and maintain such safeguards.

e. Evaluate and adjust the institution's information security program in light of the results of the testing and monitoring required by paragraph c above; any material changes to the institution's operations or business arrangements; or any other circumstances that the institution's managers know or have reason to know that may have a material impact on the institution's information security program (16 CFR section 314.4)."

Complications

Unprecedented Treatment

As a recipient of federal funding, there are many information system controls in federal laws and regulations that states must adhere to and this is the first time we are aware of OMB requiring auditors conducting a single audit to test compliance with these requirements. We conducted a word search for the names and acronyms of the following well-known federal requirements in the 1,622 page June 2016 Compliance Supplement:

- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Federal Information System Controls Audit Manual (FISCAM)
- Tax Information Security Guidelines for Federal, State and Local Agencies (Publication 1075)

Our searches of the above four requirements within the June 2016 Compliance Supplement returned zero results/hits. Additionally, a search for "information system" in the Compliance Supplement returned 27 hits. Only two of the hits relate to control activities, which are located within Part 6 for Internal Control and are not associated with the required audit objectives for a specific program.

The only current Special Tests and Provisions that we are aware of that deals with safeguards for systems relates to Medicaid titled, *ADP Risk Analysis and System Security Review*; however, its audit objective is fundamentally different from the one OMB is proposing for SFA and discussed further in the next section.

Vague Audit Objective

Part 7 of the Compliance Supplement states (bolding added):

> *"The auditor is expected to test compliance only for those requirements that are susceptible to testing by the auditor (i.e., the requirements can be evaluated against **objective criteria**, and the auditor can reasonably be expected to have sufficient basis for recognizing noncompliance)."*

Considering the term "objective criteria," here is a comparison of the audit objective proposed by OMB for Education to use for SFA to the audit objective for the ADP Risk Analysis and System Security Review used for the Medicaid program:

> **3. ADP Risk Analysis and System Security Review**
>
> **Audit Objective** – To determine whether the State Medicaid agency has performed the required ADP risk analyses and system security reviews.
>
> **14. Securing Student Information**
>
> **Audit Objectives** – Determine whether the IHE has developed, implemented, and maintained a comprehensive information security program in accordance with the Safeguards Rule.
>
> In testing the audit objective for the ADP Risk Analysis and System Security Review, all auditors can evaluate the facts of the situation and come to a conclusion on whether the state Medicaid agency has or has not performed the required ADP risk analyses and system security reviews. However, the audit objective for the Securing Student Information is written in a way that different auditors may come to different conclusions based on the facts of the situation. For example, there could be different interpretations of what is meant by a "comprehensive" information security program. Additionally, the Safeguards Rule uses terms that are subjective. The following is from Education's description of the compliance requirements for the Safeguard Rule with bolding added to emphasize items that are subjective:
>
> > *"Identify **reasonably foreseeable** internal and external risks to the security, confidentiality, and integrity of customer information that **could** result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and **assess the sufficiency** of any safeguards in place to control these risks….*
> >
> > *Evaluate and adjust the institution's information security program in light of the results of the testing and monitoring required by paragraph c above; any **material changes** to the institution's operations or business arrangements; or any other circumstances that the institution's managers know or **have reason to know that may have a material impact** on the institution's information security program."*

Additionally, part of the audit objective is not susceptible to testing by the auditor. Testing an institution's security program is at a point-in-time; however, Education is proposing that auditors provide an opinion on if the institution "maintained" an information security program in accordance with the Safeguards Rule. Unless the auditor does considerable testing throughout the audit period, the auditor would not be able to support an opinion that the institution "maintained" their information security program.

In Substance, an Opinion on Internal Controls

Additionally, Part 7 of the Compliance Supplement states (bolding added)*:*

> *"Characteristics of compliance requirements that auditors are typically expected to test include those: c. Where an audit objective can be written that supports an **opinion on compliance**."*

Auditing standards define compliance requirement as:

> *Laws, regulations, rules, and provisions of contracts or grant agreements applicable to government programs with which the entity is required to comply.*

While the Safeguards Rule falls within this definition of a compliance requirement, the Safeguards Rule appears to set internal control requirements specific to securing information systems. As a result, if an auditor issues an opinion on compliance, they will, in substance, be issuing an opinion on internal controls for an IHE's information systems. Up to this point, OMB has not required the auditor to issue an opinion on internal controls a part of a single audit nor is it required by the current audit standards, Uniform Guidance, or the Single Audit Act.

Possible Actions by OMB

Remove and Take a Measured Approach

As a result of the importance of securing information technologies, we believe that OMB should take a measured, well thought-out approach for incorporating the testing of securing information technologies into the single audit environment. It may be best for OMB to remove the new audit objective this year and not include it in future versions of the 2017 Compliance Supplement. Removing it will provide time for OMB to take a leadership role and work with federal awarding agencies, the audit community, and other stakeholders to incorporate the testing of securing information technologies into the single audit environment. We recommend that OMB work with the audit community to ensure that any future audit objectives related to cybersecurity, if any, can be consistently executed by all auditors to ensure the high-quality audits. Additionally, as OMB may be aware, the AICPA is currently working on an audit guide about *Auditing Cybersecurity in an Attestation Examination Engagement*, which OMB may want to consider as it develops future audit objectives for a single audit.

Rewrite the New Audit Objective

If OMB determines it cannot remove the new audit objective, OMB should work with Education to rewrite the audit objective so that it contains only objective criteria. To help ensure better audit understanding and consistency, the audit objectives and suggested audit procedures should provide more succinct guidance as to the nature and extent of the audit tests Education expects auditors to perform, and include specific compliance objectives that should be tested when reviewing an IHE's documented information security program. As they are currently written, the suggested audit procedures are not answerable in "YES/NO" responses as you would expect for compliance. If clarification is made as to what is required, it may be that compliance can be tested, instead of controls.

OMB may have to look within the Safeguards Rule to find objective criteria that all auditors can consistently test to determine if the auditee achieved compliance. For example, OMB could use the following as the audit objective for 2017:

> **Audit Objectives** – Determine whether the IHE designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.
>
> **Suggested Audit Procedures**
>
> a. Verify that the IHE has designated an individual to coordinate the information security program.
> b. Obtain the IHE risk assessment and verify that it addresses the three required areas noted in 16 CFR 314.4 (b).
> c. Obtain the documentation created by the IHE that aligns each safeguard with each risk identified from step b above, verifying that the IHE has identified a safeguard for each risk.

We believe this audit objective and the suggested audit procedures would be a good first start because it provides objective criteria. Additionally, findings of non-compliance, if any, would inform Education of which IHEs have not made an organizational commitment to securing student information.

Potential Ramifications if Left Unchanged

If OMB removes the new objective or rewords it as discussed above, then the issue of not supporting an opinion on compliance is resolved. However, if OMB decides to include the same wording from the draft in the final 2017 Compliance Supplement, we believe that an opinion on internal controls, in substance, is now a required part of the audit of SFA. As a result, OMB and Education should notify all IHEs of the ramifications the new audit objective could have on their 2017 single audits and beyond, which could result in one or more of the following:

Disclaimer of Opinion:

The current audit objective requires the auditor to obtain audit evidence to determine if the auditee "**maintained** a comprehensive information security program" (bolding added). If the auditor is not able to find audit evidence on the strength of the IHE's information security program throughout the audit period, then the auditor would be required to issue a disclaimer of opinion in relation to the audit objective. Given that most states are more than halfway through their fiscal year 2017, if IHEs have not already been recording and retaining documentation to support the assertion that they have maintained a comprehensive information security program, then the auditor may not be able to verify that the information security program was maintained throughout all of the audit period. If OMB releases the audit objective as written, OMB should remind IHE of their obligation to provide their auditor with documentation to support their assertion that the IHE maintained a comprehensive information security program throughout the audit period. Additionally, OMB should inform IHEs that if they are not able to provide this support, they might receive a disclaimer of opinion from their auditor.

Endless Scope:

Additionally, because securing information technologies relies on the general controls of the information system, the audit objective is unclear as to what level (at the entity-wide, system, and application levels) the auditor would be required to test general controls to be able to opine on the audit objective. *Standards for Internal Control in the Federal Government* (Green Book) states (bolding added):

> *11.07 Information system general controls (**at the entity-wide, system, and application levels**) are the policies and procedures that apply to all or a large segment of an entity's information systems. General controls facilitate the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.*

If OMB does not edit the new audit objective, an auditor may have to scope in and sample from all systems at an IHE to obtain sufficient appropriate evidence to verify that the IHE is securing student information. If OMB releases the audit objective as written, OMB should inform all IHEs that auditors may have to scope in all systems containing student information, which could potentially include systems containing information on alumni.

Re-procurement of Audit Services:

As required by 200.508, auditees must procure or otherwise arrange to obtain an auditor that can properly perform the testing required in a single audit. If OMB does not edit the wording before it is released, the auditee would need to obtain an auditor that, in substance, can provide an opinion on the IHE's controls securing their information technologies. As a result, OMB should let IHEs know that

if their current auditor is not able to provide this audit service, the auditee would need to re-procure their audit services for the fiscal year 2017 single audit. Additionally, OMB should remind IHEs that when procuring audit services, the objective is to obtain high-quality audits and they should evaluate the auditor's relevant experience in auditing information systems.

Additional Audit Costs:

We have concerns regarding the nature of this testing and the expertise of staff that is necessary to perform and understand the suggested audit procedures along with the additional cost that it would pose to auditees. This testing would likely require the services of an IT audit specialist which would significantly increase the cost of the SFA program's audit. Individual Google searches for "average salary for a CPA" and "average salary for an IT auditor" returned $65,055 and 73,670, respectively. If OMB decides to release the audit objective as written, OMB should first conduct further analysis of the skill set required to meet the audit objective and the market value for those skills. OMB should share this information with IHEs so they can budget for the potential increase in audit costs and can determine which source of funding they will use to meet this new requirement.