program to verify that the institution applied the appropriate clock to credit hour conversion formula.

c. For the sample of programs identified in procedure b, using the correct number of credit hours (as determined in procedure b), evaluate each program's eligibility, using Appendix B as a guide, considering the students allowed to be admitted to the program, mode of delivery requirements for content, and mode of delivery requirements for time.

d. Through review of ED approvals, identify any short-term programs (at least 300 clock hours but less than 600 clock hours) and substantiate the school's calculation of its completion and placement rates by (1) selecting a random sample of the regular students who were enrolled during the award year for which the most recent completion rate was calculated and testing to verify if each student in the sample was included appropriately in each step of the rate's calculation, as described in 34 C.FR 668.8(f); and (2) selecting a random sample of the students who graduated during the award year for which the most recent placement rate was calculated and testing to verify if each student in the sample was included appropriately in each step of the rate's calculation, as described in 34 CFR 668.8(g).

12. Gramm-Leach-Bliley Act–Student Information Security

SFA - Title IV Programs

Compliance Requirements The Gramm-Leach-Bliley Act (Pub. L. No. 106-102) (GLBA) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data (16 CFR 314). The Federal Trade Commission considers Title IV-eligible institutions that participate in Title IV Educational Assistance Programs as "financial institutions" and subject to the Gramm-Leach-Bliley Act because they appear to be significantly engaged in wiring funds to consumers (16 CFR 313.3(k)(2)(vi)). Institutions agree to comply with GLBA in their Program Participation Agreement with ED. Institutions must protect student financial aid information, with particular attention to information provided to institutions by ED or otherwise obtained in support of the administration of the Federal student financial aid programs (16 CFR 314.3; HEA 483(a)(3)(E) and HEA 485B(d)(2)). ED provides additional information about cybersecurity requirements at https://studentprivacy.ed.gov/security. ED also issued an Electronic Announcement on GLBA compliance that can be found at Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements | Knowledge Center.

On December 9, 2021, the FTC issued final regulations for 16 CFR Part 314 to implement the GLBA information safeguarding standards that institutions must implement. These regulations significantly modified the requirements that institutions must meet under GLBA. The regulations established minimum standards that institutions must meet. The FTC stated that it "believes many of the requirements set forth in the

Final Rule are so fundamental to any information security program that the information security programs of many financial institutions will already include them if those programs are in compliance with the current Safeguards Rule." Institutions are required to be in compliance with the revised requirements no later than June 9, 2023.

Institutions are required to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts. The regulations require the written information security program to include nine elements for institutions with 5,000 or more customers, (16 CFR 314.3(a)). The written information security program for institutions with fewer than 5,000 customers must address seven elements (16 CFR 314.3(a) and 16 CFR 314.6). In the preamble to the Final Rule, the FTC stated, "Proposed § 314.4 [Elements] altered the current Rule's required elements of an information security program and added several new elements." The FTC also stated, "[t]he elements for the information security programs set forth in this section [16 CFR 314.4} are high-level principles that set forth basic issues the programs must address, and do not prescribe how they will be addressed." The elements that an institution must address in its written information security program are at 16 CFR 314.4. At a minimum, an institution's written information security program –

Element 1
- Designates a qualified individual responsible for overseeing and implementing the institution's information security program and enforcing the information security program in compliance (16 CFR 314.4(a)).

Element 2
- Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (as the term customer information applies to the institution) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks (16 CFR 314.4(b)).

Element 3
- Provides for the design and implementation of safeguards to control the risks the institution identifies through its risk assessment (16 CFR 314.4(c)). At a minimum, the institution's written information security program must address the implementation of the minimum safeguards identified in 16 CFR 314.4(c)(1) through (8). The eight minimum safeguards that the written information security program must address are summarized as follows:
    - Implement and periodically review access controls. .
    - Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted.
    - Encrypt customer information on the institution's system and when it's in transit.
    - Assess apps developed by the institution
    - Implement multi-factor authentication for anyone accessing customer information on the institution's system
    - Dispose of customer information securely
    - Anticipate and evaluate changes to the information system or network.
    - Maintain a log of authorized users' activity and keep an eye out for unauthorized access.

Element 4
- Provides for the institution to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 CFR 314.4(d)).

Element 5
- Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program (16 CFR 314.4(e)(1)).

Element 6
- Addresses how the institution will oversee its information system service providers (16 CFR 314.4(f)).

Element 7
- Provides for the evaluation and adjustment of its information security program in light of the results of the required testing and monitoring; any material changes to its operations or business arrangements; the results of the required risk assessments; or any other circumstances that it knows or has reason to know may have a material impact the institution's information security program (16 CFR 314.4(g)).

The first element that an institution's written information security program must address is the designation of an individual with responsibility for implementing and enforcing an institution's written information security program. The regulations refer to this individual as the Qualified Individual. If an institution has not designated a Qualified Individual, it is not in compliance with the GLBA requirements. The Qualified Individual, has ultimate responsibility and accountability for implementing and enforcing the institution's information security program (16 CFR 314.4(a)). The regulations do provide for an institution to use a service provider as the Qualified Individual. In cases where an institution uses a service provider as the Qualified Individual, the institution must –

- Retain responsibility for compliance with GLBA;
- Designate a senior member of its personnel responsible for direction and oversight of the Qualified Individual; and
- Require the service provider or affiliate to maintain an information security program that protects the institution in accordance with the requirements of the regulations at 16 CFR Part 314(a)(1) through (3).

Because the written information security program may be in one or more readily accessible parts and the Qualified Individual is responsible for implementing and monitoring the information security program, it is ED's expectation that the Qualified Individual would be able to provide the written information security program that addresses the elements required for the written information security program to the auditors.

Audit Objectives Determine whether the institution designated a Qualified Individual responsible for implementing and monitoring the institution's information security program.

Determine whether the institution's written information security program addresses the required minimum seven elements.

Suggested Audit Procedures

a. Verify that the institution has designated a Qualified Individual responsible for implementing and monitoring the institution's information security program.

b. Verify that the institution has a written information security program and that the written information security program addresses the remaining six required minimum elements.

13. Federal Perkins Loan Liquidation

SFA - Title IV Programs

Compliance Requirements For an institution that decided to stop participating in the Federal Perkins Loan program (Perkins) (Assistance Listing 84.038), the institution is responsible for returning any unspent funds (34 CFR section 668.14(b)(25)). The institution must perform the end-of-participation procedures in which it must (a) notify ED of the intent to stop participating in Perkins (34 CFR section 668.26(b)(1)); (b) purchase any outstanding loans left in its Perkins portfolios or assign them to ED (34 CFR sections 674.8(d), 674.17(a)(2), and 674.45(d)(2)); and (c) maintain program and fiscal records of all Perkins funds since the most recent Fiscal Operations Report (FISAP) was submitted, and reconcile this information at least monthly (34 CFR section 674.19(d)). The FISAP form is available at https://fsapartners.ed.gov/knowledge-center/topics/campus-based-processing-information/fisap-form-and-instructions.

ED has compiled its guidance on the Perkins loan program wind-down, liquidation, and related issues at https://fsapartners.ed.gov/knowledge-center/library/program/Perkins%20Loan. In addition to the Guide, the website also includes a Federal Perkins Loan Frequently Asked Questions | Knowledge Center and other information. The website is updated by ED as additional guidance is developed.

Audit Objectives Determine whether the institution ceasing to participate in the Perkins loan program has properly performed end-of-participation procedures.

Suggested Audit Procedures

a. Review, evaluate, and document procedures that the institution used to notify ED of its intent to liquidate its Perkins loan portfolios.

b. If the institution has completed the liquidation of its Perkins loan portfolio, ascertain that the institution has either purchased or assigned to ED any Perkins loans with outstanding balances.

c. If the process of liquidating outstanding loans has not been completed, verify that the institution has begun to assign those loans to ED.