United States Government Accountability Office

Report to the Committee on Oversight and Government Reform, House of Representatives

September 2018

CYBERSECURITY

Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information

GAO-18-518

September 2018

CYBERSECURITY

Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information

GAO Highlights

Highlights of GAO-18-518, a report to the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

FSA administers billions of dollars in student financial aid, including loans and grants, to eligible college students. The processing of student aid is complex, and FSA relies on non-school partners to carry out various activities supporting the student aid process, such as loan repayment and collection.

GAO was asked to review how FSA ensures the protection of PII by its non-school partners. The objectives of this review were to (1) describe the roles of non-school partners and the types of PII shared with them and (2) assess the extent to which FSA policies and procedures for overseeing the non-school partners' protection of student aid data adhere to federal requirements, guidance, and best practices.

To address these objectives, GAO collected and reviewed FSA documentation, reports, policies, and procedures and compared FSA policies and procedures to four key practices included in federal guidance for overseeing the protection of PII by non-federal entities. GAO also interviewed FSA officials with responsibility for the oversight of non-school partners.

What GAO Recommends

GAO is making six recommendations to FSA to ensure that its oversight of non-school partners addresses the four key practices for ensuring the protection of PII. FSA concurred with three of the recommendations, partially concurred with two, and did not concur with one. It also described actions planned or under way to implement four of the recommendations. GAO maintains that all of its recommendations are warranted.

View GAO-18-518. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The Department of Education's Office of Federal Student Aid (FSA) partners with various entities ("non-school partners") that are involved primarily in supporting the repayment and collection of student loans.

- **Federal loan servicers** are responsible for collecting payments on loans and providing customer service to borrowers on behalf of the Department of Education through its Direct Loan program.
- **Private collection agencies** collect on loans that are in default and work with borrowers to help them get out of default.
- **Guaranty agencies** insure lenders against loss due to borrower default and carry out a variety of loan administration activities.
- **Federal Family Education Loan lenders** are non-federal lenders, such as banks, credit unions, or other lending institutions, that made loans to students in the past and continue to service these loans.

FSA shares a variety of personally identifiable information (PII) on borrowers with its non-school partners. This includes names, addresses, phone numbers, email addresses, Social Security numbers, and financial information.

Key practices for overseeing the protection of PII shared with non-federal entities include requiring (1) risk-based security and privacy controls, (2) independent assessments to ensure controls are effectively implemented, (3) corrective actions to address identified weaknesses in controls, and (4) ongoing monitoring of control status. FSA established oversight policies and procedures for loan servicers and private collection agencies that generally address these key practices. However, FSA exercises minimal oversight of lenders' protection of student data (see table).

Extent to Which Federal Student Aid Processes Address Key Practices for Overseeing the Protection of Personally Identifiable Information

Non-school partner	Security and privacy controls	Independent assessments	Corrective actions	Ongoing monitoring
Loan servicers	●	●	●	◐
Private collection agencies	●	●	●	◐
Guaranty agencies	◐	●	●	○
Federal Family Education Loan Lenders	◐	○	○	○

Key: ● = FSA provided evidence of processes and procedures that addressed all aspects of the key practice; ◑ = FSA provided evidence of processes and procedures that addressed some but not all aspects of the key practice; ○ = FSA did not provide evidence of processes and procedures that addressed the key practice

Source: GAO analysis of Federal Student Aid data. | GAO-18-518

FSA officials maintain that the lenders are subject to other legal and regulatory requirements for protecting customer data. However, FSA does not have a process for ensuring lenders are complying with these requirements, and thus lacks assurance that appropriate risk-based safeguards are being effectively implemented, tested, and monitored.

Contents

Figure

Abbreviations

Direct Loan	William D. Ford Direct Loan Program
FFEL	Federal Family Education Loan
FISMA	Federal Information Security Modernization Act of 2014 and still-in-effect provisions of the Federal Information Security Management Act of 2002
FSA	Office of Federal Student Aid
FTC	Federal Trade Commission
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	personally identifiable information
POA&M	plan of action and milestones
SAIG	Student Aid Internet Gateway

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 17, 2018

The Honorable Trey Gowdy
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Department of Education's Office of Federal Student Aid (FSA) is tasked with administering and overseeing billions of dollars in federal student aid,[1] including grants and loans to millions of eligible college students each year. The processing of federal student aid is complex, and FSA relies heavily on third parties, primarily to help manage student loans, including loan servicers, guaranty agencies, private collection agencies, and lenders (collectively referred to as "non-school partners"). To carry out their functions, these entities are responsible for storing and protecting large amounts of personally identifiable information (PII)[2] of students and parents that apply for and receive student aid.

You asked us to conduct a study to examine how FSA ensured protections were placed on the PII being shared with its non-school partners as part of the federal student aid process. The objectives of our review were to (1) describe the roles of FSA's non-school partners in the federal student financial aid program, including the types of PII shared with them; and (2) assess the extent to which FSA's policies and procedures for overseeing non-school partners' protection of federal student aid data align with federal requirements, federal guidance, and best practices.

To address our first objective, we obtained and reviewed documentation that discussed the federal student aid process and the types of information collected, used, and shared in the process. Specifically, we reviewed reports from the Department of Education and FSA, the

[1]Federal student aid includes loans, grants, and work-study funds to students attending college or career school.

[2]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date, and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

Congressional Research Service, and GAO regarding the federal student financial aid program and the roles of non-school partners in the program. We also reviewed FSA privacy impact assessments[3] and system documentation to identify what PII can be accessed by, or is shared with non-school partners, and through what methods. Lastly, we interviewed relevant officials from FSA who were involved in administering the student aid program.

To address the second objective, we identified key practices for overseeing the protection of PII by reviewing laws, including the Federal Information Security Modernization Act of 2014 (FISMA),[4] Office of Management and Budget (OMB) requirements and guidance on managing federal information,[5] and National Institute of Standards and Technology (NIST) information security standards and guidance.[6] We then reviewed and analyzed the policies, procedures, and processes FSA has in place for overseeing non-school partners' protection of student aid data and compared them to these practices for overseeing the protection of PII.

[3]A privacy impact assessment is an analysis of how information is handled to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

[4]The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[5]OMB, Circular A-130: *Managing Information as a Strategic Resource*, Appendices I and II (July 2016).

[6]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication 800-37, Revision 1 (Gaithersburg, Md.: February 2010); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013); *Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems*, FIPS Pub. 199 (Gaithersburg, Md.: February 2004); *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171, Revision 1 (Gaithersburg, Md.: December 2016); and *Framework for Improving Critical Infrastructure Cybersecurity*, version 1 (Gaithersburg, Md.: February 2014).

We supplemented our analyses of policies, procedures, and processes with interviews of FSA officials with knowledge of, and responsibility for the oversight of non-school partners, as well as a review of relevant Department of Education inspector general reports. A more detailed discussion of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from June 2017 to September 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

FSA seeks to ensure that all eligible individuals enrolled in postsecondary education can benefit from federal financial aid for education. It is responsible for implementing and managing programs authorized under the Higher Education Act of 1965, as amended. Specifically, Title IV of the act authorizes the federal student assistance programs for which FSA is responsible.[7] These programs (Title IV programs) provide loans, grants, and work-study funds to students attending college or career school. In fulfilling its program obligations, FSA is responsible for managing and overseeing almost $1.4 trillion in outstanding loans.

In administering Title IV programs, FSA performs a variety of functions across the student aid life cycle. These include

- educating students and families about the process of obtaining financial aid;
- processing millions of student aid applications;
- disbursing billions of dollars in aid;
- enforcing financial aid rules and regulations;
- servicing millions of student loans and helping borrowers avoid default;

[7]Title IV of the Higher Education Act (20 U.S.C. §§ 1070-1099d) authorizes programs that provide financial assistance to students attending a variety of postsecondary schools.

- securing repayment from borrowers who have defaulted on loans;
- partnering with schools, lenders, and guaranty agencies to prevent fraud, waste, and abuse; and
- insuring billions of dollars in guaranteed student loans previously issued by financial institutions.

In carrying out these functions, FSA collects, maintains, and shares a large amount of information, including sensitive personal information from students and their families. The office also relies on various automated systems to assist with student aid functions. Further, FSA works with various entities, such as loan servicers, guaranty agencies, private collection agencies, and lenders, to carry out loan servicing and collection activities.

Federal Student Financial Aid Programs

The three main categories of federal student financial aid are loans, grants, and federal work-study. Loans are student aid funds that are borrowed to help pay for eligible education programs and must be repaid with interest. FSA administers loans under the William D. Ford Direct Loan Program (Direct Loan) and the Federal Family Education Loan (FFEL) Program, along with other programs, such as Perkins Loans,[8] for students demonstrating financial need.

Direct Loans are loans for which the Department of Education is the lender. They include

- **subsidized loans** made to undergraduate students based on financial need, for which the government does not generally charge interest while the student is in grace or deferment status;[9]

[8]Under the Federal Perkins Loan Program, loans were made by schools to undergraduate and graduate students who demonstrated financial need. Participating schools operated revolving funds from which new loans are made. The funds were created through federal appropriations and institutional matching contributions. However, no new federal appropriations have been provided for many years, and the program ended on September 30, 2017, without reauthorization.

[9]For direct subsidized loans disbursed between July 1, 2012, and July 1, 2014, the borrower is responsible for paying any interest that accrues during the grace period. If the interest is not paid during the grace period, the interest will be added to the loan's principal balance.

- **unsubsidized loans** made to undergraduate and graduate students for which the borrower is fully responsible for paying interest regardless of loan status;
- **PLUS loans** made to graduate or professional students and parents of dependent undergraduate students for which the borrower is fully responsible for paying the interest regardless of the loan status; and
- **consolidation loans**, which allow the borrower to combine existing federal student loans into a single new loan.

FFEL loans are loans that were obtained through private lenders, with federal subsidies ensuring that private lenders earned a certain yield on the loans they made. Under this program, the Department of Education entered into agreements with guaranty agencies to insure the private lenders against losses due to a borrower's default. Federal law ended the origination of these loans as of July 1, 2010; however, FSA, lenders, and guaranty agencies continue to service (i.e., handle billing and other activities related to loan repayment) and collect outstanding FFEL loans. According to FSA, borrowers' eligibility is the same under both the Direct Loan and FFEL programs.

The department also administers student aid through grants, such as Pell grants,[10] which are student aid funds that generally do not have to be repaid. It also administers the federal work-study program, which provides part-time jobs for students with financial need, allowing them to earn money to help pay educational expenses.

In fiscal year 2017, FSA reported disbursing about $122.5 billion in aid to students through its various programs. In addition, the portfolio of outstanding FFEL loans totaled approximately $305.8 billion, as of September 30, 2017.[11] Table 1 provides details on the amounts of financial aid disbursed to students in fiscal year 2017 across all financial aid programs.

[10]Federal Pell Grants are awarded to undergraduate students with demonstrated financial need.

[11]According to FSA, the FFEL portfolio is located in multiple places, with about $180 billion held by FFEL lenders, about $30 billion in defaulted loans held by guarantors, and the remainder serviced by the Department of Education.

Table 1: Federal Financial Aid Disbursed to Students, Fiscal Year 2017

Dollars in millions

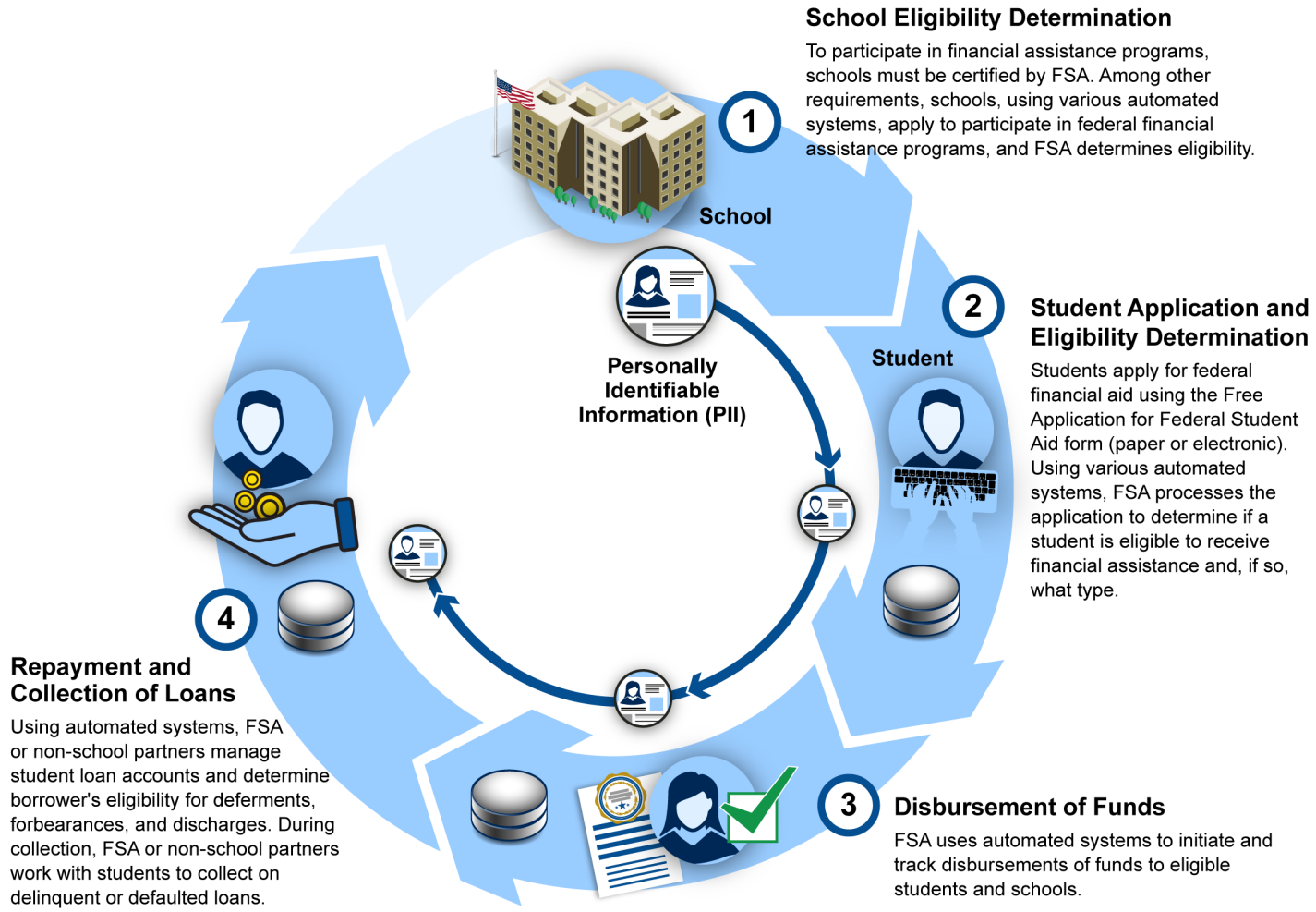
Programs	FY 2017 aid disbursed to students
Loan programs (excluding Federal Family Education Loan)	
Direct Loan	92,957
Perkins Loan	885
Grant programs	27,712
Work-study programs	949
Total	**122,503**

Source: Office of Federal Student Aid 2017 annual report. | GAO-18-518

Overview of the Financial Aid Process

The federal financial aid process is complex and consists of four phases: school eligibility determination, student application and eligibility determination, disbursement of funds, and repayment and collection of loans. Each phase of the process is supported by automated FSA information systems that collect and process student aid information. The information is then used by FSA, schools, and other stakeholders to determine the type and amount of aid a student is eligible to receive, and to support the distribution and repayment of loans. See figure 1 for an overview of the four phases.

Figure 1: Overview of the Four Phases of the Federal Student Financial Assistance Process Administered by the Department of Education's Office of Federal Student Aid (FSA)



Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-518

Federal Requirements for Protecting Information and Systems

Federal laws and guidance specify requirements for protecting federal systems and data. This includes systems used or operated by a contractor or other organization on behalf of a federal agency.

FISMA is intended to provide a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets, as well as the effective oversight of information security risks. The act requires each agency to develop,

document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency, including those provided or managed by another entity.

The primary laws that provide privacy protections for personal information accessed or held by the federal government are the Privacy Act of 1974 and the E-Government Act of 2002.[12] These laws describe, among other things, agency responsibilities with regard to protecting PII.

The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[13] It requires, among other things, that agencies issue system of records notices to notify the public when the agencies establish or make changes to a system of records. System of records notices are to identify, among other things, the types of data collected, the types of individuals about whom information is collected, the intended "routine" uses of the data, and procedures that individuals can use to review and correct personal information.

In addition, the E-Government Act of 2002 requires agencies to conduct assessments of the impact on privacy from using information systems to collect, process, and maintain PII.[14] A privacy impact assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system.

In accordance with FISMA, OMB is responsible for the oversight of agencies' information security policies and practices.[15] OMB establishes requirements for federal information security programs and assigns

[12]Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, *codified at* 5 U.S.C. § 552a (Dec. 31, 1974). E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).

[13]A system of records is a collection of information about an individual under control of an agency from which information is retrieved by the name of an individual or other identifier. 5 U.S.C. § 552a(a)(4)&(5).

[14]Pub. L. No. 107-347 § 208.

[15]44 U.S.C. § 3553.

agency responsibilities to fulfill the requirements of statutes such as FISMA.[16]

OMB requires agencies to oversee the implementation of security and privacy controls by contractors and other non-federal entities that collect, use, process, store, maintain, and disseminate federal information on behalf of a federal agency. OMB notes that agencies are ultimately responsible for ensuring that federal information is adequately protected, commensurate with the risk resulting from the unauthorized access, use, disclosure, modification, or destruction of such information. Accordingly, OMB guidance states that, when sharing PII with contractors or other non-federal entities, agencies should establish requirements for the protection of their data in written agreements with these entities.[17] For specific technical direction, OMB requires agencies to implement standards and guidelines established by NIST.

FISMA also assigns certain responsibilities to NIST, including to develop standards and guidelines for systems other than national security systems. These standards and guidelines include (1) standards for categorizing agency information and systems to provide appropriate levels of information security, according to a range of risk levels; (2) guidelines for the types of information and systems to be included in each category; and (3) minimum information security requirements for information and systems in each category.

Accordingly, NIST has developed a series of information security standards and guidelines for agencies to follow in managing information security risk. NIST guidance provides steps that agencies can take to identify appropriate security and privacy controls and establish specific requirements for implementing those controls to ensure consistency both internally and externally to the agency. NIST guidance also outlines requirements for protecting the confidentiality of controlled unclassified information (which includes PII) when it resides in a non-federal system or organization. Relevant publications include the following:

[16]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: July 2016).

[17]OMB, Circular A-130: *Managing Information as a Strategic Resource*, Appendices I and II (July 2016).

- Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*,[18] requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values from among the security categories that the agency identifies for each type of information residing on those information systems.
- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*,[19] provides a catalog of security and privacy controls for federal information systems and organizations. It also provides a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the nation from a diverse set of threats. These threats include hostile cyber attacks, natural disasters, structural failures, and human errors. The guidance includes privacy controls to be used in conjunction with the specified security controls to achieve comprehensive security and privacy protection. According to NIST, the privacy controls are based on the Fair Information Practice Principles[20] embodied in the Privacy Act of 1974, the E-Government Act of 2002, and OMB policies.
- NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*,[21] explains how to apply a risk management framework to federal information systems, including security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

[18]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

[19]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4 (Gaithersburg, Md.: April 2013).

[20]The Fair Information Practice Principles are widely accepted in the United States and internationally as a general framework for privacy and are reflected in other federal and international laws and policies.

[21]NIST*, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37 Revision 1 (Gaithersburg, Md.: February 2010).

- NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*,[22] provides federal agencies with recommended security guidance for protecting the confidentiality of controlled unclassified information[23] when it resides in a non-federal system and organization.
- The *Framework for Improving Critical Infrastructure Cybersecurity*,[24] serves as a baseline for protecting critical information assets. It is intended to help organizations apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. The framework outlines a risk-based approach to managing cybersecurity that is composed of three major parts: a framework core, profile, and implementation tiers.

Subsequent to the issuance of the NIST cybersecurity framework, a May 2017 executive order required agencies to use the framework to manage cybersecurity risks.[25] It also outlined actions to enhance cybersecurity across federal agencies and critical infrastructure to improve the nation's cyber posture and capabilities against cybersecurity threats to digital and physical security.

In addition, the Gramm-Leach-Bliley Act requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data.[26] As part of its implementation of the act, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions under FTC's jurisdiction to have measures in place to keep customer information secure.[27]

[22]NIST, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, SP 800-171 (Gaithersburg, Md.: December 2016).

[23]Controlled unclassified information is unclassified information throughout the executive branch that requires any safeguarding or dissemination control, which includes PII.

[24]NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1 (Gaithersburg, Md.: February 2014).

[25]Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017); 82 Fed Reg. 22391 (May 16, 2017).

[26]Sections 501-502, Title V, subtitle A, Pub.L. No. 106-102 (Nov. 12, 1999); 15 U.S.C. §§ 6801-6802.

[27]16 C.F.R. Part 314.

Specifically, the rule requires financial institutions to develop a documented information security program that describes the administrative, technical, or physical safeguards used to protect customer information. The program must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its program, each company must

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement information safeguards to control risks and regularly monitor and test their effectiveness;
- select service providers that can maintain appropriate safeguards, require them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

GAO Previously Highlighted the Need to Improve Policies and Procedures for the Protection of Student Aid Data

We recently reported on aspects of FSA's protection of student aid data, noting that weaknesses existed in key processes. Specifically, in November 2017, we reported, among other things, that FSA needed to improve its policies and procedures for the management and protection of student aid data.[28] For example, while the agency had established policies and procedures for key privacy requirements, such as publishing notices to describe how personal information is to be maintained, used, and accessed, it did not always ensure that privacy impact assessments for its information systems included an analysis of privacy risks and mitigation steps.

In addition, we reported that FSA's information security policies and procedures were not always up to date. Further, we noted that the agency

[28]GAO, *Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information*, GAO-18-121 (Washington, D.C.: Nov. 27, 2017).

needed to strengthen its oversight of schools' implementation of federal information security requirements to help ensure student aid information was adequately protected.

We recommended that the Secretary of Education take seven actions to strengthen FSA's management and protection of federal student aid records and enhance its oversight of schools. For example, we recommended that the agency incorporate information security program requirements in its reviews of postsecondary schools, and that the Department of Education update its regulation to include protections of personal information as an element of a school's ability to demonstrate its administrative capability. FSA concurred or generally concurred with five of our seven recommendations, partially concurred with one recommendation, and did not concur with another.

Non-School Partners Play Key Roles in the Federal Student Aid Process and Have Access to Large Amounts of Personally Identifiable Information to Facilitate Their Activities

FSA's non-school partners play key roles in the federal student financial aid program, particularly with regard to the servicing,[29] repayment, and collection of student loans. These partners include FFEL lenders, Title IV loan servicers, guaranty agencies, and private collection agencies. FSA shares a variety of PII with the non-school partners to assist them in carrying out their functions.

[29]Loan servicing includes sending bills to borrowers and collecting loan payments after the loan has entered repayment.

FSA's Non-School Partners Perform Key Roles Related to Loan Servicing, Repayment, and Collection

Non-school partners are involved primarily in the loan servicing, repayment, and collection phases of the federal student aid process.

- **FFEL lenders:** During the administration of the FFEL program, these lenders were involved primarily in the disbursement of funds.[30] As part of the program, students and parents obtained federal loans through non-federal lenders, such as the borrower's school, a bank, credit union, or other lending institution. Generally, lenders provided the loan proceeds to a student's school, which then credited the student's account and disbursed the residual amount, if any, to the student.[31]

  After a loan was disbursed, lenders chose to either service the loan, contract with an outside organization for servicing, or sell the loan. According to FSA, the majority of lenders have third-party servicers that perform servicing, billing, and reporting on their behalf. The lenders also work closely with guaranty agencies, which insure FFEL loans in case of default, and oversee certain aspects of the lenders' activities. As of June 2018, there were 1,079 lenders participating in the FFEL program.[32]

  Although FSA purchased a portion of the FFEL loans as a result of disruptions in financial markets during the financial crisis of 2007 and 2008, the majority of the FFEL portfolio continues to be owned and serviced by private lenders. These lenders are required to report quarterly on their portfolios and are to sign participation agreements with FSA requiring that electronic data submitted by the lenders be accurate and conform to applicable laws, regulations, and policies. FSA also noted that lenders are regulated by a variety of entities, such as the FTC, Federal Deposit Insurance Corporation, Federal Reserve, Department of the Treasury, and, in some cases, state agencies.

- **Title IV loan servicers:** These organizations are primarily involved in the repayment and collection phase of the aid process. Under the Direct Loan program, after the loan is disbursed, the Department of

[30]Under the Higher Education Act, eligible FFEL lenders include banks, postsecondary schools, credit unions, and state nonprofit agencies.

[31]The residual amount is the amount of loan proceeds remaining after the school collects tuition, fees and, if applicable, room and board.

[32]While the Health Care and Education Reconciliation Act of 2010 ended the origination of new FFEL loans as of July 1, 2010, lenders continue to hold, service, and collect outstanding FFEL loans.

Education contracts with loan servicers to perform a variety of administrative functions.[33] Loan servicers are responsible for collecting payments on a loan, advising borrowers on resources and benefits to better manage their federal student loan obligations, responding to customer service inquiries, and performing other administrative tasks associated with maintaining a loan on behalf of the Department of Education.

In addition, once a Direct Loan becomes delinquent (i.e., the first day after a borrower fails to make a scheduled monthly payment), loan servicers may take several actions pending the loan entering default, such as reaching out to past-due borrowers and entering into repayment arrangements for loans. As of July 2018, FSA contracted with 11 loan servicers.[34]

The contracts between FSA and the servicers establish the servicers' responsibilities in the aid process. The contracts lay out requirements for servicers with regard to financial reporting, internal controls, accounting, and other areas.

- **Guaranty agencies:** These agencies are state or private non-profit entities that are primarily involved in the repayment and collection phase of the aid process. As part of the FFEL program, they receive federal funds to play the lead role in administering aspects of the program. These agencies' functions include insuring private lenders against losses due to a borrower's default or other losses (the guaranty agencies are, in turn, reinsured by the federal government);[35] providing assistance in preventing delinquent borrowers from going into default; working with defaulted student and parent borrowers to rehabilitate their defaulted loans, restore their credit, and provide them with a fresh start; and reporting actions to credit bureaus.

  Prior to July 2010, when the origination of FFEL loans stopped, guaranty agencies also were involved in verifying student eligibility for loans and notifying lenders, who would send a promissory note to lenders for their signature and disburse the funds. According to FSA,

[33]Direct Loan servicers may also service federally held FFEL program loans.

[34]Prior to 2009, FSA had a single loan servicer for the Direct Loan program. Beginning in 2009, FSA entered into contracts with additional loan servicers, awarded as part of a strategy to improve performance by fostering competition among servicers.

[35]With federal funding, guaranty agencies generally provide insurance to the lenders for 98 percent of the unpaid principal of defaulted loans.

guaranty agencies continue to work closely with holders of FFEL loans, including supporting them in default aversion activities and overseeing aspects of their operations through monitoring, auditing, and ensuring compliance with regulations. As of July 2018, 24 guaranty agencies were administering FFEL loans.

FSA uses participation agreements to govern the agencies' responsibilities in the aid process. The agreements lay out reporting requirements, records retention periods, and other requirements. For example, guaranty agencies are required to report to the Department of Education on the loans they insure. They are also required to keep records and have them available for inspection by the federal government.

- **Private collection agencies:** Private collection agencies are also primarily involved in the repayment and collection phase of the aid process. If borrowers default on their loans after entering the repayment phase, private collection agencies will attempt to enter into voluntary repayment agreements, while ensuring that defaulted borrowers are aware of both the consequences of their failure to repay and the options available to help them get out of default.[36]

  Other debt resolution functions performed by private collection agencies include determining whether a borrower's account is eligible for administrative resolutions, such as discharge due to death or total and permanent disability; determining whether a borrower's account is eligible for involuntary payment methods such as administrative wage garnishment; preparing accounts for litigation; and returning accounts to FSA for failure to convert the account to active repayment status. As of July 2018, FSA had contracts with 18 private collection agencies. These contracts describe the private collection agencies' responsibilities in the aid process.

[36]Loans are in default if a borrower has not made a payment for 270 days (9 months), and the borrower has not made arrangements with their lender or servicer such as a deferment or forbearance.

FSA Shares Extensive Amounts of Personally Identifiable Information about Borrowers with Non-School Partners

In administering the federal student aid program, FSA shares a large amount of PII that it collects from students and parents with its non-school partners. This is particularly significant in that FSA directly manages or oversees more than 203 million student loans made to approximately 43 million borrowers. PII collected when students or their parents apply for financial aid includes, but is not limited to the following:

- **Student demographics:** Name, address, Social Security number, telephone numbers, email address, marital status, driver's license number, etc.
- **Student eligibility:** Citizenship status, dependency status, high school completion status, selective service registration (if applicable), and whether the student has a drug conviction, among other information.
- **Student finances:** Tax return filing status; adjusted gross income; cash, savings, and checking account balances; untaxed income; and current net worth of student's assets.
- **Parent demographics (if applicable):** Name, Social Security number, email address, and marital status.
- **Parent finances:** Tax return filing status, adjusted gross income, tax exemptions, and asset information.

After the borrower's eligibility is determined or the funds are disbursed, the PII that the agency collected as part of the process is stored on several of FSA's internal IT systems.

FSA shares the PII stored on its systems with its non-school partners to assist them in carrying out their respective functions. This sharing occurs when the agency grants non-school partners access to specific systems. According to FSA, the data that non-school partners have access to depends on the non-school partner's relationship with the individual holding the loan. Table 2 provides a description of the FSA systems from which non-school partners receive student aid data, as well as the types of PII they contain.

Table 2: Federal Student Aid (FSA) Systems Used to Share Student Aid Data with Non-School Partners and the Personally Identifiable Information They Contain

System	Description	Types of personally identifiable information contained in this system	Non-school partners with access
Central Processing System	Processes all applications for FSA, calculates financial aid eligibility, and notifies students and educational institutions of the results of the eligibility calculation.	Student demographics, student eligibility, student finances, parent demographics, parent finances	Guaranty agencies[a]
Common Origination and Disbursement system	Initiates and tracks the disbursement of funds to eligible students and schools for financial aid programs.	Student demographics, student finances, parent demographics, parent finances	Title IV loan servicers
Debt Management and Collection System	Allows FSA partners to store, retrieve, and edit debtor information and process payments on defaulted accounts.	Student demographics, student finances, parent demographics, parent finances	Private collection agencies, Title IV loan servicers
National Student Loan Data System	Provides a centralized, integrated view of federal student aid loans and tracks them through their entire life cycle.	Student demographics, student eligibility, student finances, parent demographics, parent finances	Lenders, Title IV loan servicers, and guaranty agencies

Source: GAO analysis of FSA information. | GAO-18-518

[a]According to FSA, since new loans were not originated under the Family Federal Education Loan program after 2010, guaranty agencies no longer have access to this system.

To gain access to FSA systems and data, non-school partners must submit an application to use FSA's Student Aid Internet Gateway (SAIG). The SAIG application enables the enrolling organization (i.e., the non-school partner) to select services to receive, submit, view, and/or update student financial aid data online, or receive or send information by batch exchange. To gain access to services allowing them to receive, submit, view, and update student aid data, each non-school partner must designate a Primary Data Point Administrator, who is responsible for determining which staff within the non-school partner's organization are to be given access to FSA's systems and data. The primary Data Point Administrator is also responsible for ensuring the privacy of the information obtained or provided via the SAIG.[37]

[37]The SAIG application states that information provided to Data Point Administrators by the department is protected by the Privacy Act of 1974 as amended. In addition, FSA has published system of records notices describing how personal information in its systems is to be maintained, used, and accessed.

According to FSA officials, enrollment for access to borrower data via the SAIG varies based on the type of non-school partner and the functions it performs. Further, the officials stated that non-school partners can only access information about the borrowers with whom they are directly involved. The services that non-school partners can access via the SAIG include the following:

- **Central Processing System data:** Processed data from the Free Application for Federal Student Aid are reported to institutions on the Institutional Student Information Record, and corrections to data can be made.[38]
- **Common Origination and Disbursement System data:** Origination, disbursement, and other required reporting information for the Direct Loan program can be exchanged electronically between FSA and non-school partners.
- **National Student Loan Data System:** Title IV, enrollment history information, and federal grant information can be viewed and updated by non-school partners.
- **Financial Management System:** Financial reporting information can be sent by non-school partners to FSA.

FSA's Oversight of Non-School Partners' Protection of Student Aid Data Is Inconsistent

As noted previously, OMB and NIST guidance calls for agencies to oversee third-party entities with which they share PII to ensure that appropriate security and privacy controls are in place.[39] This guidance identifies key practices for overseeing the protection of data by such entities. These practices include the following, among others:

- **Require the implementation of risk-based security and privacy controls:** NIST guidance states that agencies should categorize their

[38]As previously noted, as of 2010, guaranty agencies no longer have access to this system, and other non-school partners were not provided with access.

[39]OMB, Circular A-130; NIST, SP 800-37, Rev. 1; NIST, FIPS PUB 199; NIST, SP 800-53, Rev. 4; NIST, SP 800-171; and NIST, *Framework for Improving Critical Infrastructure Cybersecurity*.

information and systems based on their risk impact level[40] and require the implementation of security controls that include one of three baseline sets of controls that correspond to the impact level, tailored to the system and organization as appropriate.[41]

- **Independently assess the implementation of security controls:** Security control assessments determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome. For external entities that store or process federal information, NIST guidance states that agencies can verify that controls have been implemented through independent, third-party assessments or attestations.[42]
- **Develop and implement corrective actions:** As part of the process for conducting security control assessments, organizations should develop remedial actions to address identified weaknesses and track them to closure.[43]
- **Monitor the implementation of controls on an ongoing basis:** Ongoing monitoring includes ensuring that technical, management, and operational security controls are tested at an organization-defined frequency and results are provided to officials on an ongoing basis. NIST guidance notes that agencies should monitor security control compliance by external entities on an ongoing basis.[44] This can be achieved through reporting the security status of the system and security controls on an ongoing basis.[45]

FSA has established policies and procedures for overseeing its non-school partners' protection of the PII that it shares with the partners. These policies and procedures vary in the extent to which they address

[40]FIPS 199 defines the categorization of information or an information system based on an assessment of the potential impact (low, moderate, or high) that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. The impact level of the information is used in turn to assign an impact level to the system containing that information, and the corresponding selection of a baseline of security controls.

[41]NIST, FIPS Publication 200: *Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, Md.: March 2006).

[42]NIST SP 800-53.

[43]NIST SP 800-37.

[44]NIST SP 800-53.

[45]NIST SP 800-37.

the key practices for overseeing the protection of PII. For example, FSA's policies and procedures for Title IV loan servicers and private collection agencies fully address three of the four key practices. For guaranty agencies, FSA's procedures require onsite assessments but do not require monitoring controls on an ongoing basis. Finally, for FFEL lenders, FSA has minimal oversight procedures.

FSA Established Security Requirements for Loan Servicers and Private Collection Agencies

FSA established policies and procedures for overseeing Title IV loan servicers and private collection agencies that generally address the key selected practices for overseeing the protection of data. Specifically, by applying its standard contractor oversight processes, the agency has addressed three of the four key practices that pertain to loan servicers and private collection agencies. FSA partially addressed one practice related to ensuring that the implementation and effectiveness of all controls is monitored on an ongoing basis. Table 3 summarizes the extent to which FSA's processes address the key practices for loan servicers and private collection agencies.

Table 3: Extent to Which the Office of Federal Student Aid's (FSA) Processes for Overseeing Loan Servicer and Private Collection Agency Protection of Student Aid Data Address Key Oversight Practices

	Require risk-based security and privacy controls	Independently assess the implementation of controls	Develop and implement corrective actions	Monitor controls on an ongoing basis
Loan servicers	●	●	●	◐
Private collection agencies	●	●	●	◐

Legend:

● = FSA provided evidence of processes and procedures that addressed all aspects of the key practice

◑ = FSA provided evidence of processes and procedures that addressed some but not all aspects of the key practice

○ = FSA did not provide evidence of processes and procedures that addressed the key practice

Source: GAO analysis of FSA information. | GAO-18-518

FSA required loan servicers and private collection agencies to implement risk-based security and privacy controls: FSA established security requirements and guidance for loan servicers and private collection agencies. These requirements are communicated through provisions in the contracts that FSA has with the loan servicers and private collection agencies. Specifically, FSA requires loan servicers and private collection agencies to implement security controls in accordance

with NIST's *Security and Privacy Controls for Federal Information Systems and Organizations*.[46]

The contracts also require loan servicers and private collection agencies to adhere to applicable Department of Education and FSA security policies and procedures. For example, the Department of Education's policy for security system categorization, which applies to contractor-owned systems (such as those owned by loan servicers and private collection agencies), requires that systems containing PII be categorized as, at a minimum, "moderate impact."[47] This categorization reflects an assessment of the risks associated with a compromise of the information and determines the selection of appropriate security controls for the information system.

In addition, FSA developed a standard operating procedure for implementing security requirements based on this determination, which applies to loan servicers and private collection agencies. This process for categorizing systems and selecting and implementing controls is based on NIST's risk management framework, including steps for selecting, implementing, and assessing controls, and authorizing the information system to operate.[48]

FSA required independent assessments of the implementation of security controls: To help ensure that loan servicers and private collection agencies meet minimum security standards, FSA developed procedures for assessing the implementation of security controls based on applicable federal guidance. Specifically, FSA's security authorizations process includes procedures for an independent assessor to review security controls implemented on the loan servicers' and private collection

[46]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (April 2013).

[47]According to NIST, information or systems should be categorized as "moderate impact" if the loss of confidentiality, integrity, or availability might be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. See NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199 (Gaithersburg, Md.: February 2004).

[48]NIST defines authorization to operate as the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.

agencies' systems.[49] This includes, among other things, developing a test plan; executing the plan, to include observing security controls; running automated scans; and collecting artifacts and evidence. The independent assessor then is to document the issues, findings, and recommendations for remediation.

According to FSA's procedures, once the assessment of the loan servicer's or private collection agency's system is completed, issues have been identified, and a plan of action and milestones (POA&M) has been developed, an FSA authorizing official is to review key documentation and make a decision on whether to authorize the system to operate. This decision is to be based on a determination as to whether the residual risk to agency operations, agency assets, resources, or individuals resulting from the operation of the system is acceptable. Once approved, the authorization to operate the system is valid for 3 years, provided that the conditions, if any, specified in the POA&M are met.

FSA established a process for developing and implementing corrective actions: FSA requires loan servicers and private collection agencies to follow a standard operating procedure for documenting and implementing corrective actions to address weaknesses identified during security assessments. This procedure requires the owners of the systems to work with their agencies' information system security officers and FSA's internal independent validation and verification teams to document deficiencies and remediation plans in the FSA's POA&M management tool, review and document evidence to close deficiencies, and provide monthly updates on the status of POA&Ms, along with reasons for any overdue items. FSA officials added that they are reviewing ways to further automate the process for flagging overdue items.

In addition, the procedure specifies time frames for system owners to remediate weaknesses based on their criticality. To confirm that a weakness has been addressed, the procedure requires FSA's independent validation and verification team to review submitted plans and evidence and determine if they are sufficient to close the deficiency.

[49]A security control assessor is the individual, group, or organization responsible for conducting a security control assessment, which is the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

FSA did not fully establish a process for monitoring all controls on an ongoing basis: To monitor security controls between the independent assessments supporting the authorization to operate process, FSA's contracts with loan servicers require the servicers to have a continuous monitoring program, as defined by NIST SP 800-37. Similarly, FSA's contracts with private collection agencies require these agencies to enroll their systems in FSA's Continuous Security Authorization program, which is intended to oversee and monitor the security controls in FSA's information systems on an ongoing basis.

In addition, the contracts require the private collection agencies to ensure that independent testing and monitoring of system security controls is performed on an ongoing basis. The contracts require these tests to cover a subset of the system security controls quarterly so that all controls are tested at least once during a 3-year period.

However, according to FSA Technology Office officials, neither loan servicers nor private collection agencies have been enrolled in FSA's Continuous Security Authorization program, as required. The officials added that they had not established a time frame to incorporate loan servicers and private collection agencies into the agency's continuous monitoring program.

According to the officials, both loan servicers and private collection agencies rely on their own continuous monitoring programs to oversee their systems; however, only the private collection agencies report the results of their monitoring activities to FSA (on a quarterly basis). In addition, FSA does not specify which controls the loan servicers and private collection agencies are to test; rather, it leaves this determination to the non-school partners.

FSA policy also requires that loan servicers and private collection agencies respond to an annual self-assessment questionnaire concerning their implementation of NIST security and privacy controls. According to the FSA officials, if deficiencies are noted in the agencies' responses, FSA works with the non-school partners to create POA&Ms and track remediation efforts through closure.

Officials in FSA's Technology Office added that loan servicers participate in FSA's Web Application Surveillance Program, in which FSA conducts vulnerability scans of the servicers' systems and shares findings with the servicers for remediation on a monthly or quarterly basis, depending on the environment being tested.

Nevertheless, while these processes can provide helpful information about the loan servicers' and private collection agencies' security posture on an ongoing basis, they do not ensure that all security controls implemented on these partners' systems are tested on a regular basis. For example, according to FSA policy, the Web Application Surveillance Program is intended to simulate the scanning and probing of a web application that might be useful to intruders. However, the program is not intended to ensure that management, operational, and technical controls have been implemented.

Without fully establishing policies and procedures for ongoing monitoring of security controls implemented by loan servicers and private collection agencies, FSA has less assurance that these controls are effectively implemented and operating as intended. Further, FSA has a limited ability to ensure that risks associated with these non-school partners' use of PII have been adequately mitigated.

FSA Established Security Requirements for Guaranty Agencies, but Lacks a Process for Ongoing Monitoring of Controls

FSA policies and procedures requires guaranty agencies to implement security and privacy controls to protect student aid data, and the agency has recently enhanced its processes to include independent, on-site assessments of those controls and the development of corrective actions for identified weaknesses. However, it lacks processes for monitoring guaranty agencies' implementation of controls on an ongoing basis. Table 4 summarizes the extent to which FSA's processes address the four key practices for overseeing the protection of data by guaranty agencies.

Table 4: Extent to Which the Office of Federal Student Aid's (FSA) Processes for Overseeing Guaranty Agency Protection of Student Aid Data Address Key Oversight Practices

	Require risk-based security and privacy controls	Independently assess the implementation of controls	Develop and implement corrective actions	Monitor controls on an ongoing basis
Guaranty agencies	◐	●	●	○

Legend:

● = FSA provided evidence of processes and procedures that addressed all aspects of the key practice

◑ = FSA provided evidence of processes and procedures that addressed some but not all aspects of the key practice

○ = FSA did not provide evidence of processes and procedures that addressed the key practice

Source: GAO analysis of FSA information. | GAO-18-518

FSA did not fully specify a required baseline of risk-based security and privacy controls for guaranty agencies: FSA requires, through written agreements, that guaranty agencies participating in the federal

student aid program comply with federal security requirements. Specifically, these agreements include an amendment that requires the guaranty agencies to ensure that any information systems that include PII about borrowers implement security and privacy controls specified in NIST guidance.[50]

In addition, when applying for access to FSA systems and information through the SAIG, guaranty agencies agree to protect the privacy of all information that has been provided by the Department of Education. In particular, guaranty agencies are required to affirm that administrative, operational, and technical security controls are in place and operating as intended.

FSA provides guidance to guaranty agencies on implementing security controls, in the form of a template to be used in completing an annual self-assessment (discussed in more detail below). This template identifies security and privacy controls to be used in the self-assessment, based on the NIST control baseline for moderate-impact systems. The guaranty agencies are expected to inform FSA as to whether they have implemented these controls.

However, the agreements FSA has established with guaranty agencies do not specify that information must be maintained at a specific impact level or that guaranty agencies are to implement a particular baseline set of security controls that correspond to an agency established risk-based impact level. As noted previously, once agencies determine the impact level of their information or systems, they should select one of three baselines of security controls (low, moderate, or high) that correspond to the impact level. This baseline can then be tailored based on risk and the specific organizational and system environment.

According to FSA officials, the agreements allow the guaranty agencies to determine whether their systems are low, moderate, or high impact. The officials also added that guidance provided to guaranty agencies, such as self-assessment questionnaires—are based on the NIST 800-53 moderate baseline.

However, allowing guaranty agencies to determine the specific designation could result in inconsistent implementation of security

[50]This includes NIST SP 800-53, revision 4.

controls if guaranty agencies choose varying impact levels for their systems. OMB guidance states that agencies should require third parties with whom PII is shared to maintain security at a specified impact level. By not specifying in written agreements the impact level of the information it shares with guaranty agencies, and a corresponding set of minimum security requirements, FSA jeopardizes its ability to ensure that the PII it shares with guaranty agencies will be adequately and consistently protected.

FSA established a process for on-site assessment of guaranty agencies' security and privacy controls: Prior to fiscal year 2018, FSA relied on a self-assessment process, wherein guaranty agencies completed annual questionnaires about their implementation of security and privacy controls. The completed questionnaires were reviewed by FSA staff, who then met with guaranty agency staff over the telephone to discuss any identified weaknesses. As part of this process FSA staff did not collect or review documentation to independently verify whether controls had been appropriately implemented, or conduct on-site reviews to obtain first-hand evidence of the implementation of the controls. However, according to FSA officials, they also conducted targeted, on-site visits to selected guaranty agencies in 2016 and 2017 to verify security control implementation.

FSA has recently enhanced its process for assessing guaranty agencies' implementation of security and privacy controls. FSA officials stated that, in March 2018, they began a series of on-site assessments of guaranty agencies which are to be completed by the end of September 2018. FSA provided the guaranty agencies with a security plan template that outlines roles and responsibilities, methodology, controls to be tested, and the test plan approach for these assessments. In addition, the list of evidence includes required artifacts to demonstrate compliance with NIST requirements.

FSA officials stated that they plan to alternate between on-site assessments and self-assessments each year. By enhancing its approach to assessing guaranty agencies' implementation of security requirements, FSA should be better positioned to ensure that the data shared with these entities are being adequately protected.

FSA processes include monitoring of guaranty agency corrective actions: As part of the guaranty agency self-assessment process, FSA established procedures for documenting weaknesses identified during the self-assessments and corrective action plans for addressing the

weaknesses. FSA Deputy Chief Information Officer officials stated that they track the corrective action plans in a system that provides weekly status reports that include notifications of overdue corrective actions. The officials added that all actions to correct weaknesses identified during the self-assessments were to be taken within 12 months of identifying the corrective actions.

In April 2018, FSA officials stated that they intended to follow a procedure similar to the one used for the self-assessments to document and monitor corrective actions for weaknesses identified during the on-site assessments of guaranty agencies' security and privacy controls. Specifically, the officials noted that all findings of weaknesses during the on-site assessments are to be turned into POA&Ms, assigned an expected completion date, and tracked to completion by FSA. This procedure, if effectively implemented, should help FSA ensure that gaps in security controls are remediated in a timely manner.

FSA did not establish a process for monitoring all guaranty agency controls on an ongoing basis: To monitor guaranty agencies' compliance between assessments, FSA officials stated that they hold weekly teleconferences with officials from guaranty agencies during which they discuss new security requirements or other issues. FSA Information Technology officials stated that they follow up with guaranty agencies after these calls to ensure that they implement new requirements. In addition, FSA issued guidance to guaranty agencies in January 2018 on conducting vulnerability scans of these agencies' systems. This guidance addresses vulnerability testing guidelines and scanning requirements, as well as guidance on security control testing.

However, FSA does not monitor all security controls by requiring guaranty agencies to report regularly on the status of security controls between on-site assessments. Neither the weekly teleconferences nor the vulnerability scans include testing the implementation of all security and privacy controls on a defined, periodic basis or reporting results to FSA.

FSA officials stated that they rely on the on-site and self-assessments to oversee guaranty agencies' security control implementation because FSA does not have a contractual relationship with guaranty agencies and does not own the guaranty agencies' systems. However, OMB and NIST note that agencies have a responsibility for ensuring that their information is protected at a consistent level even when such information is shared with non-federal partners. Without fully establishing procedures for ongoing monitoring of guaranty agencies, FSA cannot fully ensure that risks to the

student aid data containing PII that it shares with guaranty agencies have been adequately mitigated.

FSA Exercises Minimal Oversight of FFEL Lenders' Protection of Student Aid Data

FSA established high-level requirements for FFEL lenders to protect student aid data, but it exercises minimal oversight to ensure implementation of security and privacy protections for these data. Table 5 summarizes the extent to which FSA's processes for overseeing lenders address key practices for overseeing the protection of data.

Table 5: Extent to Which the Office of Federal Student Aid's (FSA) Processes for Overseeing Federal Family Education Loan Lender Protection of Student Aid Data Address Key Oversight Practices

	Require risk-based security and privacy controls	Independently assess the implementation of controls	Develop and implement corrective actions	Monitor controls on an ongoing basis
Federal Family Education Loan Lenders	◐	○	○	○

Legend:

● = FSA provided evidence of processes and procedures that addressed all aspects of the key practice

◑ = FSA provided evidence of processes and procedures that addressed some but not all aspects of the key practice

○ = FSA did not provide evidence of processes and procedures that addressed the key practice

Source: GAO analysis of FSA information. | GAO-18-518

FSA did not fully specify risk-based security and privacy controls for FFEL lenders: Like other non-school partners, lenders must complete FSA's SAIG application when applying for access to FSA data and systems. The SAIG application outlines general requirements for ensuring the security and privacy of the data that FSA shares with the lenders.

In addition, FFEL lenders enter into participation agreements with FSA which include requirements related to data exchange, such as ensuring that data lenders share with FSA are correct. Also, FSA officials told us that security requirements are communicated to the lenders' staff via "dear colleague" letters and the security notices that appear when users log on to the agency's Access and Identity Management System to access PII and other data.[51]

[51]This system is FSA's security solution that manages access to the online elements of systems. It allows users of FSA systems to log in using their FSA user ID, password, and their SAIG mailbox number (where applicable).

However, neither the SAIG application nor the participation agreement requires the FFEL lenders to implement a baseline set of risk-based security and privacy controls based on the impact level of the affected information and systems. FSA Information Technology and Business Operations officials said that they plan to add security and privacy requirements to the FFEL lender participation agreements as part of their next update during the 2018 revision cycle, but they did not specify what requirements would be included in these revised agreements. Until FSA establishes specific requirements for lenders' protection of data, it will lack assurance that information it shares is being protected in a manner consistent with FSA's determination of its sensitivity.

FSA did not require independent assessments of FFEL lenders' implementation of controls: FSA does not have policies or procedures for independently assessing lenders' implementation of protections for student aid data. The SAIG application does not require an independent assessment of the non-school partners' information security and privacy controls to determine the extent to which the controls are implemented correctly, operating as intended, or producing the desired outcome with respect to security.

According to FSA officials, by accepting the terms of use displayed when logging on to FSA systems, users agree to comply with security and privacy requirements. The officials added that FSA monitors activity on the National Student Loan Data System and can remove a user's access if a case of improper usage is identified. However, FSA's procedures for monitoring system usage do not include an independent assessment of lenders' implementation of security controls.

Further, while FFEL lenders may be required to undergo various compliance audits and program reviews, FSA has not determined the extent to which these audits or reviews address security and privacy protections; it also does not review the results of such reviews to gain assurance that security and privacy protections are in place. Without requiring evidence of such assessments, FSA does not have a basis for ensuring that lenders are implementing adequate security and privacy protections.

FSA has not established a process for overseeing corrective actions taken by FFEL lenders: Since FSA does not require independent assessments of lenders' information security controls, it does not have a process for identifying weaknesses in the FFEL lenders' security and privacy controls and monitoring corrective actions. Lenders do not notify

FSA of security or privacy weaknesses that may be identified in their systems, nor do they report on corrective actions taken to remedy such weaknesses. In the absence of such reporting, FSA cannot ensure that weaknesses in the security and privacy controls of the lenders' systems are being addressed.

FSA did not establish procedures for monitoring FFEL lenders' implementation of controls on an ongoing basis: FSA does not have a process for ongoing monitoring of lenders' implementation of security or privacy safeguards. FSA does not require lenders to provide periodic reports to FSA on their security and privacy posture or to conduct any reviews of their implementation of security and privacy controls. Without requiring evidence that lenders are effectively implementing security and privacy protections, FSA cannot ensure that the data accessed by lenders are being safeguarded commensurate with risk.

Regarding the lack of FFEL lender oversight, FSA officials noted that lenders, as financial institutions, are subject to a number of other legal and regulatory requirements that were not defined by FSA as part of the FFEL program. For example, lenders are subject to requirements for protecting customer information imposed by the Gramm-Leach-Bliley Act and FTC's Safeguards Rule, which calls for financial institutions to document an information security program that includes specific elements.

However, FSA does not have a process for ensuring that lenders are complying with these, or other, requirements related to the protection of student aid data. Consequently, FSA lacks assurance that risk-based safeguards commensurate with the sensitivity of these data are being effectively implemented, tested, and monitored. In our previous work, we similarly found that FSA did not have assurance that schools, which are also required to comply with the FTC Safeguards Rule, were implementing these requirements.[52]

OMB noted that agencies are ultimately responsible for ensuring that their information is adequately protected, and NIST stated that this responsibility does not change when information is shared with non-federal partners.[53] Accordingly, agencies should have assurance that

[52]GAO-18-121.

[53]See OMB A-130, Appendices I and II and NIST SP 800-171.

information they share with non-federal entities is being protected at an appropriate level. In the case of FSA, this could include leveraging processes already in place, such as the FTC Safeguards Rule, to gain assurance that appropriate security and privacy controls are in place and are being regularly monitored and tested. Without establishing a process for gaining such assurance, FSA is not meeting its responsibility to ensure that borrowers' data are being adequately protected.

Conclusions

FSA shares PII on millions of people with non-school partners (i.e., loan servicers, private collection agencies, guaranty agencies, and FFEL lenders) so that they can carry out key aspects of the federal student aid program. FSA is responsible for ensuring that its non-school partners protect this information by implementing adequate information security and privacy safeguards.

While FSA has taken steps to oversee the security and privacy protections of some of its non-school partners, its policies and procedures did not always include all key oversight practices. In particular, while FSA established requirements for loan servicers and private collection agencies, along with processes for ensuring their implementation that generally adhered to the key practices, the agency had not ensured that controls are tested and results are reported on an ongoing basis. FSA, therefore, may lack visibility into the effectiveness of the protections applied to student aid data.

With respect to guaranty agencies, FSA established security and privacy requirements and has taken steps to enhance security assessments. Nevertheless, without ensuring that controls are monitored on an ongoing basis, it lacks adequate assurance that security controls required by FSA are in place and effective.

Further, because it exercised minimal oversight over FFEL lenders, FSA has limited assurance that they are protecting student aid data consistent with the agency's requirements. FSA's limited oversight could result in inconsistent or ineffective implementation of security controls, which in turn could have serious consequences for the privacy of millions of borrowers whose information is shared with non-school partners.

Recommendations for Executive Action

We are making the following six recommendations to the Department of Education:

- The Secretary of Education should enroll loan servicers in FSA's continuous monitoring program and, in the interim, require these entities to report the results of security controls testing at an FSA-defined frequency.

  (Recommendation 1)

- The Secretary of Education should enroll private collection agencies in FSA's continuous monitoring program, and, in the interim, require these entities to test all controls at an FSA-defined frequency and regularly report the results.

  (Recommendation 2)

- The Secretary of Education should modify FSA's agreements with guaranty agencies to specify a required baseline of security controls based on the impact level of the information shared with these agencies, as determined by FSA.

  (Recommendation 3)

- The Secretary of Education should establish a process for continuous monitoring of guaranty agencies' implementation of security and privacy requirements between on-site assessments, to include testing all controls at an FSA-defined frequency and regularly reporting results.

  (Recommendation 4)

- The Secretary of Education should include specific security and privacy requirements in agreements with FFEL lenders based on FSA's categorization of the information shared with the lenders.

  (Recommendation 5)

- The Secretary of Education should develop policies and procedures to gain assurance that FFEL lenders have appropriate security and privacy controls in place and that these controls are being regularly tested and monitored.

  (Recommendation 6)

Agency Comments and Our Evaluation

We received written comments on a draft of this report from FSA. In its comments (reprinted in appendix II), FSA concurred with three of our recommendations, partially concurred with two recommendations, and did not concur with one. In addition, FSA provided technical comments, which we have incorporated as appropriate.

FSA generally concurred with our first three recommendations and described various actions it planned or had under way to implement them. Specifically, regarding our recommendation to enroll loan servicers in FSA's continuous monitoring program (recommendation 1), the agency stated that loan servicers are scheduled to be enrolled in its ongoing security authorization program beginning in fiscal year 2019.

Regarding our recommendation to enroll private collection agencies in FSA's continuous monitoring program and, in the interim, require these entities to test all controls at an FSA-defined frequency and regularly report the results (recommendation 2), FSA stated that it concurred, although the actions it said it planned to take would not fully address the recommendation. Specifically, the agency stated that it intends to work with private collection agencies to identify specific relevant criteria to strengthen continuous monitoring testing schedules and include these criteria in private collection agencies' quarterly reports to FSA. This measure, if implemented effectively, would address the interim measure called for in our recommendation.

However, FSA did not describe actions to address the first part of our recommendation. Specifically, it did not state whether it intended to enroll private collection agencies in its ongoing security authorization program, as called for by its contracts with these agencies. Doing so would provide enhanced oversight of their implementation of security and privacy controls.

The agency concurred with our recommendation to modify FSA's agreements with guaranty agencies to specify a required baseline of security controls (recommendation 3). In this regard, FSA stated that the agreements it has established with guaranty agencies require them to comply with standards in NIST Special Publication 800-53, revision 4, and that assessments of the guaranty agencies require compliance with the moderate-impact level control baseline under the applicable NIST standards. Even though FSA did not describe plans to modify its agreements with guaranty agencies to explicitly require a specific baseline of controls, the procedures that it noted should help FSA ensure

that guaranty agencies are protecting student aid data based on the office's determination of risk. We intend to follow up with FSA to obtain and assess the evidence supporting its implementation of these recommendations.

FSA stated that it partially concurred with two other recommendations. With respect to establishing a process for continuous monitoring of guaranty agencies' implementation of security and privacy requirements between on-site assessments, to include testing all controls at an FSA-defined frequency and regularly reporting results (recommendation 4), FSA cited its process for on-site assessments or self-assessments as the means by which it monitors guaranty agencies. Specifically, it stated that it requires guaranty agencies to annually either complete a self-assessment or participate in an on-site assessment.

However, FSA did not describe any additional steps it intends to take to monitor guaranty agencies' implementation of security and privacy controls between assessments. As noted in the report, the self-assessment process that FSA established for guaranty agencies does not include such elements as collecting or reviewing documentation to verify that controls have been appropriately implemented. Further, FSA does not monitor all security controls between on-site assessments by requiring guaranty agencies to report regularly on the status of security controls. Regular reporting on the status of security controls, such as test results, would provide FSA with additional assurance that guaranty agencies have implemented adequate protections. Thus, we believe our recommendation remains appropriate.

FSA also stated that it partially concurred with our recommendation to include specific security and privacy requirements in agreements with FFEL lenders based on FSA's categorization of the information shared with the lenders (recommendation 5). Specifically, FSA stated that it has revised its 2019-2020 Lender Organization Participation Agreement with FFEL lenders to include specific security and privacy responsibilities and requirements, which is to be effective at the beginning of fiscal year 2019. The planned actions that the agency described in its response should fully address our recommendation, if effectively implemented. We intend to follow up with FSA to obtain and assess the evidence supporting its implementation of this recommendation.

FSA did not concur with our recommendation to develop policies and procedures to ensure that FFEL lenders have appropriate security and privacy controls in place and that these controls are being regularly tested

and monitored (recommendation 6). According to the agency, it lacks statutory authority under the Higher Education Act to monitor FFEL lenders in this area. FSA noted that the lenders are already subject to security and privacy controls that are monitored and enforced through other legal authorities that are not administered by the Department of Education or FSA.

However, we continue to believe that our recommendation should be implemented. We recognize that FSA may not have the authority to impose additional requirements related to monitoring the adequacy of security and privacy controls implemented by FFEL lenders. Furthermore, the recommendation does not require FSA or the Department of Education to exercise additional regulatory authority over FFEL lenders or to conduct testing or other assessments of the lenders' security and privacy programs. Rather, it seeks for FSA to review the results of other compliance audits or program assessments, including, as appropriate, those conducted by other federal entities, to acquire visibility into the lenders' implementation of information security and privacy safeguards. Leveraging such a process should help provide FSA with assurance that the student aid data it shares with them are being adequately protected. Accordingly, we have clarified our recommendation to better reflect its intent.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Education, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9342 or marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Nick Marinos
Director, Cybersecurity and Data Protection Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) describe the roles of the Office of Federal Student Aid's (FSA) non-school partners in the federal student financial aid program, including the types of personally identifiable information (PII) shared with them; and (2) assess the extent to which FSA's policies and procedures for overseeing non-school partners' protection of federal student aid data align with federal requirements, federal guidance, and best practices.

To address the first objective, we obtained and reviewed various documentation that described the federal student aid process and the types of information collected, used, and shared in the process. To determine the roles played by non-school partners in the federal student aid process, we reviewed reports from the Department of Education and FSA, including FSA's annual reports for fiscal years 2016 and 2017, and reports from the department's Office of Inspector General; reports from the Congressional Research Service on federal student aid programs; and prior GAO reports on aspects of federal student aid programs. These non-school partners included entities that FSA directly engages with to carry out key aspects of the student aid process. These partners were

- non-federal lenders participating in the Federal Family Education Loan program,
- Title IV loan servicers,
- guaranty agencies, and
- private collection agencies.

Specifically, we identified key functions carried out by these partners, the types of agreements they had with FSA, and the numbers of each type of partner that FSA engages with.

To determine the types of PII shared with non-school partners, we reviewed FSA documentation on key systems used to collect, store, and process information as part of the student aid process. This included high-level documentation and descriptions of FSA's systems architecture, privacy impact assessments for FSA and non-school partner systems, and information on the process by which FSA enrolls non-school partners to share student aid data with the agency. We also reviewed previous GAO reports on FSA's management of student aid data, including PII collected during the aid process. In addition, we interviewed FSA officials, including officials from the agency's technology and business operations offices.

To address the second objective, we reviewed and analyzed the policies, procedures, and processes FSA has in place for overseeing non-school partners' protection of student aid data and compared them to federal requirements and guidance for ensuring the protection of PII. We identified key activities for overseeing the protection of PII by reviewing laws, including the Federal Information Security Modernization Act of 2014;[1] Office of Management and Budget requirements and guidance on managing federal information;[2] and National Institute of Standards and Technology information security standards and guidance.[3] Based on our review of these requirements and guidance, we identified four key practices for establishing security and privacy requirements for non-federal entities and overseeing the implementation of these requirements. These practices are

- require the implementation of risk-based security and privacy controls,
- independently assess the implementation of security controls,
- develop and implement corrective actions, and
- monitor the implementation of controls on an ongoing basis.

We collected and reviewed evidence provided by FSA (policy and process documents, artifacts, written responses to questions, and verbal responses to questions) to understand its processes for overseeing the non-school partners' protection of student aid data. We then compared

[1]The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[2]OMB, Circular A-130: *Managing Information as a Strategic Resource*, Appendices I and II (July 2016).

[3]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication 800-37, Revision 1 (Gaithersburg, Md.: February 2010); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013); *Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems*, FIPS Pub. 199 (Gaithersburg, Md.: February 2004); *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171, Revision 1 (Gaithersburg, Md.: December 2016); and *Framework for Improving Critical Infrastructure Cybersecurity*, version 1 (Gaithersburg, Md.: February 2014).

the processes to the four key practices we identified. We determined whether the process met, partially met, or did not meet the key practices:

- Met – the agency provided evidence of processes and procedures that address all aspects of the key practice.
- Partially met – the agency provided evidence of processes and procedures that address some, but not all aspects of the key practice.
- Not met – the agency did not provide evidence of processes and procedures that addressed the key practice.

We supplemented our review with interviews of FSA Business Operations and Information Technology officials with knowledge of and responsibility for the oversight of non-school partners. We also reviewed relevant Department of Education inspector general reports.

We conducted this performance audit from June 2017 to September 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Office of Federal Student Aid

August 16, 2018

Mr. Nick Marinos
Director
Cybersecurity and Data Protection Issues Team
United States Government Accountability Office
Washington, D.C. 20548

Dear Mr. Marinos:

I am pleased to write on behalf of the U.S. Department of Education (Department) in response to the statements and recommendations made in the Government Accountability Office (GAO) draft report, "*Cybersecurity: Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information*" (GAO-18-518).

We appreciate the opportunity to respond to this GAO draft report. The Department agrees with GAO on the importance of protecting the security and privacy of data and personally identifiable information (PII) held by the Department's non-school partners that participate in the federal student loan programs. As noted in the draft report, GAO is aware of the Department's many established and planned updates to policies and procedures for overseeing the protection of data at non-school partners. However, the Department does not fully concur with GAO on the Department's and Federal Student Aid's (FSA's) role in overseeing the security and privacy of the data systems of our non-school partners given the complex relationships FSA has with each of these non-school partners and the legal authorities that govern those relationships. Our response to each of the six recommendations in the GAO draft report is set forth below.

Recommendation 1: The Secretary of Education should enroll loan servicers in FSA's continuous monitoring program and, in the interim, require these entities to report the results of security controls testing at an FSA-defined frequency.

Response: FSA concurs with this recommendation. Loan servicers under Title IV of the Higher Education Act as amended (HEA) are scheduled to be enrolled into FSA's ongoing security authorization program in fiscal year (FY) 2019 (October 1, 2018, through September 30, 2019). Prioritization and timeframes will be coordinated with the implementation of FSA's Next Generation Financial Services Environment (NextGen).

Recommendation 2: The Secretary of Education should enroll private collection agencies in FSA's continuous monitoring program, and, in the interim, require these entities to test all controls at an FSA-defined frequency and regularly report the results.

Response: FSA concurs with this statement to the extent that private collection agencies (PCAs) already report to FSA on a quarterly basis any deficiencies they find during their own continuous monitoring. In FY 2019, FSA will work with the PCAs to identify specific relevant criteria to

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

830 First St. N.E., Washington, DC 20202

strengthen the continuous monitoring testing schedules and request PCAs to report on these additional criteria when they report to FSA on a quarterly basis. FSA does not believe an interim measure is required.

Recommendation 3: The Secretary of Education should modify FSA's agreements with guaranty agencies to specify a required baseline of security controls based on the impact level of the information shared with these agencies, as determined by FSA.

Response: FSA concurs with this recommendation, and in fact FSA's agreements with guaranty agencies (GAs) were revised in 2015 to include a requirement that GAs must comply with the standards in National Institute of Standards and Technology (NIST) SP 800-53, Rev 4. FSA's assessments of the GAs require that GAs comply with the moderate specific security impact level under the applicable NIST standards.[1]

Recommendation 4: The Secretary of Education should establish a process for continuous monitoring of guaranty agencies' implementation of security and privacy requirements between on-site assessments, to include testing all controls at an FSA-defined frequency and regularly reporting results.

Response: FSA partially concurs with this recommendation. FSA has developed an annual monitoring process to review GAs' implementation of security and privacy requirements. This annual process requires GAs to either complete a self-assessment or to participate in an on-site assessment. In FY 2017, all GAs completed a self-assessment and in FY 2018, FSA is planning to conduct on-site assessments of all GAs. In FY 2019, FSA will conduct an on-site assessment of targeted GAs and the remaining GAs must complete a self-assessment.

Recommendation 5: The Secretary of Education should include specific security and privacy requirements in agreements with FFEL lenders based on FSA's categorization of the information shared with the lenders.

Response: FSA partially concurs with this recommendation. FSA revised the 2019-2020 Lender Organization Participation Agreement with Federal Family Education Loan (FFEL) lenders to include specific security and privacy responsibilities and requirements. FSA will implement these agreements with FFEL lenders at the beginning of FY 2019. However, as noted previously to GAO, FSA does not have the legal authority under the HEA to impose specific requirements on, or to monitor, FFEL lenders on data security. Lenders are already subject to other security and privacy requirements, including those in the Gramm-Leach-Bliley Act (GLBA).

[1] NIST SP 800-53, Rev. 4 incorporates the Federal Information Processing Standards (FIPS) Publication 199 for the security categorization process that federal agencies must use to select and specify the appropriate security controls for federal information systems and information, by determining the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. Under FIPS Publication 199, there are three security objectives for information and information systems that are assessed: confidentiality, integrity, and availability. NIST 800-61 Vol. 1, Rev. 1 provides that the confidentiality impact level for PII would generally fall into the moderate range.

Recommendation 6: The Secretary of Education should develop policies and procedures to ensure that FFEL lenders have appropriate security and privacy controls in place and that these controls are being regularly tested and monitored.

Response: FSA does not concur with this recommendation because, as noted above and previously to GAO, FSA lacks statutory authority under the HEA to monitor FFEL lenders in this area. FFEL lenders are already subject to security and privacy controls that are monitored and enforced through other legal authorities that are not administered by the Department or FSA. One such authority, the GLBA, requires FFEL lenders as "financial institutions" to explain their information-sharing practices to their customers and to safeguard sensitive data. As part of its implementation of the GLBA, the Federal Trade Commission (FTC) issued the "Safeguards Rule," which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure.

I appreciate your efforts to highlight the importance of the Department's non-school partners' implementation of security and privacy measures to protect student aid data.

Sincerely,

James F. Manning
Acting Chief Operating Officer

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Nick Marinos, (202) 512-9342, marinosn@gao.gov

Staff Acknowledgments

In addition to the contact named above, John De Ferrari (assistant director), Chris Businsky, Marisol Cruz, Rebecca Eyler, Lee McCracken, David Plocher, and Bruce Rackliff made key contributions to this report.