United States Government Accountability Office

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

November 2017

FEDERAL STUDENT AID

Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information

Accessible Version

On December 15, 2017, pg. 55 of this report was revised to add footnote 59, which corrected a statement attributed to the Department of Education's Assistant Inspector General for Audit.

GAO-18-121

November 2017

FEDERAL STUDENT AID

Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information

GAO Highlights

Highlights of GAO-18-121, a report to the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

FSA oversees the award of billions of dollars in federal student aid to eligible students each year. The processing of student aid requires FSA, along with participating schools, to perform a range of functions across the student aid life cycle, including the management of PII on students and their families.

GAO was asked to examine how FSA and schools manage federal student aid records. The objectives of this study were to: (1) describe how FSA and schools use information they collect to manage the federal student aid program, (2) determine the extent to which FSA policies and procedures for managing and protecting this information align with federal requirements, (3) describe the extent to which schools have established policies and procedures for managing student aid information, and (4) determine the extent to which FSA ensures that schools protect this information. To do this, GAO reviewed Education and FSA policies and interviewed agency officials. GAO also administered a survey to a stratified random sample of 560 schools that is generalizable to the population of about 6,200 schools.

What GAO Recommends

GAO recommends that FSA take seven actions to strengthen its management and protection of federal student aid records and enhance its oversight of schools. FSA concurred or generally concurred with five of GAO's recommendations, partially concurred with another, and did not concur with another. GAO believes all of the recommendations as discussed in the report are warranted.

View GAO-18-121. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The Department of Education's (Education) Office of Federal Student Aid (FSA) and postsecondary schools collect, use, and share a variety of information—including personally identifiable information (PII)—from students, their families, and others to support the administration of student aid. This information is used to make decisions about the eligibility of schools to participate in federal student aid programs, the processing of student applications and students' eligibility to receive various types of aid, the disbursement of funds to aid recipients, and the repayment of loans and recovery of defaulted loan payments.

Education and FSA have established policies and procedures for managing and protecting student information that are aligned with applicable federal laws. However, shortcomings in key areas hinder the effectiveness of FSA's procedures. For example, FSA established procedures and tools for managing and organizing records and scheduling them for disposition, but did not fully establish such procedures for electronic data, ensure that employees regularly received training, or conduct a required internal assessment of its records management program. Regarding the protection of student information, FSA did not consistently analyze privacy risks for its electronic information systems, and policies and procedures for protecting information systems were not always up to date. FSA's shortcomings are consistent with the Education Inspector General's identification of persistent weaknesses in the department's information security policies, procedures, and controls. Recommendations to address these weaknesses are not yet fully implemented. Until FSA implements the recommendations, it increases the risk of improper disclosure of information contained in student aid records.

Based on a GAO survey of schools, the majority (an estimated 95 percent of all schools) of those participating in the federal student aid process reported having policies in place, including records retention and disposition policies. However, schools varied in the methods they used to store records, the retention periods for paper and electronic records, and the disposition control activities they employed (such as the authorization and approval process for destroying records).

FSA oversees schools' participation in student aid programs, but this oversight does not extend to schools' information security programs. To oversee schools' compliance, FSA conducts reviews of schools' student aid programs, based on a number of risk factors. However, it has not identified implementation of information security programs as a factor to consider in selecting schools for program reviews, even though schools have reported serious data breaches. GAO's review of selected schools' policies found that schools did not always include required information security elements, such as assessing risks or designing and implementing safeguards. Moreover, Education's implementing regulations do not require schools to demonstrate their ability to protect student information as a condition for participating in federal aid programs. This raises concerns about FSA's oversight and how effectively schools are protecting student aid information. Until Education ensures that information security requirements are considered in program reviews of schools, FSA will lack assurance that schools have effective information security programs.

Contents

Tables

Figures

Abbreviations

COD	Common Origination and Disbursement
CPS	Central Processing System
Education	Department of Education
FISMA	Federal Information Security Modernization Act of 2014 and Federal Information Security Management Act of 2002
FSA	Office of Federal Student Aid
NARA	National Archives and Records Administration
NIST	National Institute of Standard and Technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information

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

November 27, 2017

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

The Office of Federal Student Aid (FSA) is a Principal Office of the Department of Education (Education) and is tasked with ensuring that all eligible students enrolled in postsecondary educational schools benefit from federal financial assistance for education and training.[1] The office oversees the award of billions of dollars in federal student aid, including low-interest loans and grants, to millions of eligible students each year. The processing of federal student aid is complex and requires FSA, along with its contractors and school partners (hereafter referred to as "schools") that manage and dispense the aid, to perform a range of functions across the student aid life cycle.[2] These functions include handling and storing personally identifiable information (PII) on students, such as Social Security numbers, dates of birth, and tax data.[3]

At your request, we conducted a study to examine how FSA and schools manage federal student aid records. Our objectives were to: (1) describe how FSA and schools use the information they collect in managing the student financial assistance program; (2) determine the extent to which FSA policies and procedures for managing and protecting federal student aid information align with federal requirements and guidance; (3) describe the extent to which schools have established policies and procedures for managing and protecting federal student aid information; and (4)

[1]The term "financial assistance" includes loans, grants, and work-study funds to students attending college or career school.

[2]By schools we mean institutions of higher education and postsecondary vocational institutions that are eligible to participate in FSA programs, provided that the institution offers the appropriate type of program.

[3]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.

determine the extent to which FSA ensures that schools protect federal student aid information in accordance with federal requirements and guidance.

To address the first objective, we obtained and reviewed documentation that described the federal student aid process and the types of information being collected, used, and shared in the process.[4] Specifically, we reviewed Education and FSA documentation, including information collection requests, system of records notices, privacy impact assessments (PIA), and descriptions of automated systems used to manage the student aid process.

For the second objective, we reviewed Education and FSA policies and procedures, as well as other standards and guidance describing the management and protection of federal student aid information. Specifically, we reviewed policies and procedures related to records management, including the storage and disposition of records; protecting the privacy of PII; and securing information systems. We compared these policies and procedures to federal requirements found in the *Federal Records Act, Privacy Act of 1974, E-Government Act of 2002*, and *Federal Information Security Modernization Act of 2014* (FISMA). We also compared the policies and procedures to regulations and guidance issued by the National Archives and Records Administration (NARA), the Office of Management and Budget (OMB), and the National Institute of Standards and Technology.

For the third objective, we developed and administered a web-based survey to a generalizable stratified random sample of 560 schools from a population of about 6,200 schools. To ensure that our survey questions were clear and logical and that a financial aid administrator or other responsible official identified by FSA could answer the questions accurately and without undue burden, we pretested the draft survey and conducted related telephone interviews with 3 schools that were part of our sample. We then incorporated their comments in finalizing our survey. The survey was administered from November 2016 through March 2017. We received responses to the survey from 349 schools, which are

[4]For the purposes of this report, we define "federal student aid" to mean money from the federal government—specifically, the U.S. Department of Education—that helps eligible students pay for the costs of attending college or career school.

generalizable to the population of schools.[5] We analyzed the schools' responses to the survey to determine how schools manage and protect student aid information.

In addition, we asked 123 schools, randomly selected from the 560 schools in our sample, to provide documentation of their policies and procedures for managing federal student aid information. Of these 123 schools, 44 submitted documentation. We assessed this documentation to determine whether the policies and procedures addressed how student aid information is accessed, used, and protected; how long student aid information is retained; how student aid information is disposed; and whether an information security program was developed in accordance with federal standards for safeguarding customer information. The results of our analysis of the school-provided documentation are not generalizable to the population of schools.

To address the fourth objective, we analyzed applicable federal laws and regulations, including the *Higher Education Act of 1965*, as amended; FSA program review documentation and compliance audit guides; the FSA fiscal year 2017 school program review instructions; and FSA program review procedures. In addition, we analyzed OMB's *Uniform Administrative Requirements*, *Cost Principles*, and *Audit Requirements for Federal Awards, 2 CFR Part 200, Appendix XI, Compliance Supplement* (hereafter referred to as OMB's *Compliance Supplement*) and the Education's Office of Inspector General's guide for audits of proprietary schools.[6] We compared the *Compliance Supplement* and the Education Office of Inspector General guide's financial statement and compliance requirements to the Federal Trade Commission's requirement for safeguarding customer information, including standards for records management, security, and privacy that independent auditors are to follow in conducting compliance audits at schools.

[5]From the 560 selected institutions we identified 21 "out of scope" schools (i.e., schools that were either closed or ineligible to provide federal student aid) and received valid responses from 349 from the 539 remaining in-scope schools. This represents an unweighted response rate of about 65 percent. All percentage estimates from our sample have margins of error at the 95 percent confidence level of plus or minus 12 percentage points or less, unless otherwise noted. See appendix I for more details.

[6]Department of Education, Office of Inspector General, *Guide for Audits of Proprietary Schools and for Compliance Attestation Engagements of Third-Party Servicers Administering Title IV Programs* (Washington, D.C.: September 2016).

For all of the objectives, we supplemented our document reviews and analyses with interviews of relevant agency officials. A more detailed discussion of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from December 2015 to November 2017 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

As a Principal Office within Education under the supervision of the department's Chief Operating Officer, FSA seeks to ensure that all eligible individuals enrolled in postsecondary education schools can benefit from federal financial assistance for education. FSA is responsible for implementing and managing the federal student financial assistance 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—referred to as "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 $1.3 trillion in outstanding loans.

In order to administer its various financial assistance programs, FSA is responsible for a range 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 financial aid applications;
- disbursing billions of dollars in student financial aid;

[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.

- enforcing financial aid rules and regulations;
- servicing millions of student loans and helping borrowers avoid default;
- securing repayment from borrowers who have defaulted on their loans;
- partnering with schools, financial institutions, and guaranty agencies to prevent program 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 the functions included in the student aid life cycle. Further, FSA works with various entities, such as lenders and guaranty agencies, to carry out loan servicing and collection activities.

FSA Financial Assistance Programs

FSA disburses billions of dollars through its financial assistance programs, also known as federal financial aid, to students. This aid covers expenses such as tuition and fees, room and board, books and supplies, and transportation. The three main categories of financial assistance programs include: (1) loans, (2) grants, and (3) 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 these loans under the William D. Ford Federal Direct Loan Program (Direct Loan), the Federal Family Education Loan Program, the Health Education Assistance Loan Program, and the Federal Perkins Loan Program.

Direct Loans include the following subtypes:

- **Direct Subsidized Loans:** Federal loans are made to undergraduate students based on financial need, on which the government does not generally charge interest while in grace or in deferment status.[8]
- **Direct Unsubsidized Loans:** Federal loans are made to undergraduate and graduate students for which the borrower is fully responsible for paying interest, regardless of loan status. Interest accrues from the date of disbursement and continues through the life of the loan.
- **Direct PLUS Loans:** Federal loans are 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 loan status.
- **Direct Consolidation Loans:** Federal loans allow the borrower to combine one or more existing federal student loans into a single new loan. The borrower only has to make one monthly payment on the consolidated loan, and the repayment term may be longer than on the original loans, which may result in a lower monthly payment.

Under the Federal Family Education Loan program, students and parents obtained federal loans through private lenders. Guaranty agencies insured lenders against borrower default, and Education, in turn, reinsured the guaranty agencies. Federal law ended the origination of these loans as of July 1, 2010; however, FSA, lenders, and guaranty agencies continue to service and collect the outstanding Federal Family Education Loans.

The third loan program, the Health Education Assistance Loan Program, provided loans between 1978 and 1998 to eligible graduate students in schools of medicine, osteopathy, dentistry, veterinary medicine, optometry, podiatry, public health, pharmacy, and chiropractic, or in programs in health administration and clinical psychology. A 1992 act of Congress ended the program on September 30, 1998.[9] On July 1, 2014, responsibility for handling loan repayments resulting from the program

[8]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.

[9]*Health Professions Education Extension Amendments* of 1992, Pub. L. 102-408 (Oct. 13, 1992).

was transferred from the Department of Health and Human Services to Education.

Finally, under the Federal Perkins Loan Program, loans were made by schools to undergraduate and graduate students who demonstrate 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.

Grants are student aid funds offered by FSA that do not have to be repaid (unless other conditions apply[10]) and may include the following types:

- **Federal Pell Grants:** Aid awarded to undergraduate students with demonstrated financial need.
- **Federal Supplemental Educational Opportunity Grants:** Grants awarded to students and administered directly by the financial aid office at participating schools. Each participating school receives a certain amount of these funds each year from FSA.
- **Teacher Education Assistance for College and Higher Education Grants:** Federal grants awarded to eligible undergraduate or graduate students who agree to teach mathematics, science, or other specialized subjects in high-need schools for at least 4 years, within 8 years of graduation.
- **Iraq and Afghanistan Service Grants:** Federal grants awarded to students who are not eligible for a Pell Grant based on financial need, but who meet the remaining Pell Grant eligibility requirements and (1) have a parent or guardian who died as a member of the U.S. armed forces as a result of military service in Iraq or Afghanistan after the events of September 11, 2001; and (2) were under 24 years old or enrolled in college at least part-time at the time of their parent's or guardian's death.

Federal Work-Study is a program that provides part-time jobs for undergraduate, graduate, and professional students with financial need,

[10]If students fail to fulfill the service requirements of a particular grant, the grants will convert to direct unsubsidized loans, with interest accrued from the time of the award.

allowing them to earn money to help pay education expenses. The program is available to full-time or part-time students and encourages community service work, often related to the student's course of study. The program is administered by the participating schools.

In fiscal year 2016, FSA reported disbursing about $125.7 billion in aid to students through its various programs (a decrease of about $3 billion from fiscal year 2015). Table 1 provides details on the amounts of financial aid disbursed to students in fiscal years 2015 and 2016 across all financial aid programs.

Table 1: Federal Financial Aid Distributed to Students, Fiscal Years 2015-2016 (dollars in millions)

	Programs	FY 2015 aid distributed to students	FY 2016 aid distributed to students	Difference	Percent increase/decrease
Loan programs	Direct Loan	95,853	94,685	(1,168)	(1.2)
	Perkins Loan	1,158	1,044	(114)	(9.8)
	Subtotal	97,011	95,729	(1,282)	(1.3)
Grant programs	Pell Grant	29,909	28,189	(1,720)	(5.8)
	Supplemental Educational Opportunity Grant	730	729	(1)	(0.1)
	Teacher Education Assistance Grants	91	90	(1)	(1.1)
	Other grant programs/rounding	—	1	1	N/A
	Subtotal	30,730	29,009	(1,721)	(5.6)
Work-study programs	Federal Work-Study	950	964	14	1.5
	Rounding	—	(1)	(1)	N/A
	Grand total	**128,691**	**125,702**	**(2,990)**	**(2.3)**

Source: Department of Education, Office of Federal Student Aid. | GAO-18-121

Participants in the Financial Assistance Programs

Throughout the federal student aid life cycle, various federal and nonfederal entities participate in the program. These entities include the students, schools, and lenders working with or on behalf of FSA.[11] They also include:

[11]As of May 2017, there were 9 loan servicers, 26 guaranty agencies, and 35 private collection agencies working with or on behalf of FSA.

- loan servicers—entities that collect payments on loans, respond to customer service inquiries, and perform other administrative tasks associated with maintaining a loan;
- guaranty agencies—state or private nonprofit entities that have agreements with Education under which they will administer a loan guarantee program under the *Higher Education Act*; and
- private collection agencies—entities that recover unpaid debt from borrowers who have defaulted on their loans.

Table 2 describes the roles and responsibilities of each entity and FSA's role and responsibility with regard to each entity.

Table 2: Entities and Roles Involved in the Federal Student Aid Process

Entity	Entity's role in federal student aid process	Office of Federal Student Aid (FSA) role
Students	Receive and repay student aid to finance their postsecondary educations	Engage with students by increasing awareness of federal student aid; providing products, services, and tools; identifying students for whom aid can make a difference; protecting them from unfair, deceptive, or fraudulent practices; and overseeing loan servicing and debt collection activities to manage the recovery of student loan funds.
Postsecondary institutions (schools)	Determine student aid packages and disburse funds	Monitor the schools' compliance, educate them regarding policy, and assist them in meeting requirements
Federal Family Education Loan holders and servicers	Hold and service outstanding loans	Monitor the loan holders' and servicers' compliance, assist them in meeting requirements, pay interest and special allowance payments, and educate them regarding policy
FSA loan servicers	Service the Direct Loan portfolio and portions of the Federal Family Education Loan portfolio; provide systems and services to support FSA operations such as applications and disbursements; and counsel borrowers on repayment options, process payments, and engage in default prevention efforts	Set performance standards and oversee the loan servicers' operations
Guaranty agencies	Insure Federal Family Education Loans and service their defaulted loan portfolio	Monitor these agencies' compliance, assist them in meeting requirements, educate them regarding policy, and pay default claims
Private collection agencies and debt management and collection systems vendor	Collect defaulted student loans	Contract with collection agencies and debt management and collection vendor and monitor their compliance with debt collection laws and contractual requirements

Source: Department of Education, Office of Federal Student Aid. | GAO-18-121

Legal Requirements for Managing and Protecting Personal Information

Several federal laws set forth requirements that federal agencies, such as Education, must comply with in collecting, managing, and protecting information, including information collected from the general public.

Paperwork Reduction Act Requirements

The *Paperwork Reduction Act* was enacted to improve the management of information resources by federal agencies and to minimize the paperwork burden for individuals; small businesses; educational and nonprofit institutions; federal contractors; state, local and tribal governments; and other persons resulting from the collection of information by or on behalf of the federal government.[12] The act generally provides that every federal agency must obtain approval from OMB before using identical questions to collect information from 10 or more persons. Once an agency decides to collect information, it must prepare an information collection request. The information collection request must (1) describe the information to be collected, (2) provide the reason the information is needed, and (3) estimate the time and cost for the public to answer the request. After reviewing the request, OMB may approve or disapprove the information collection request, or define conditions that must be met for approval.

Records Management Requirements

The *Federal Records Act* requires federal agencies to establish and maintain an active, continuing program for the economical and efficient management of the records of the agency.[13] To implement the provisions of the act, the National Archives and Records Administration has issued regulations with specific requirements.[14] These include assigning records management responsibilities; establishing program objectives, responsibilities, and authorities for the creation, maintenance, and disposition of agency records; integrating records management and

[12]44 U.S.C. § 3501.

[13]44 U.S.C. §§ 3101 and 3102.

[14]36 C.F.R. §§ 1220–1239.

archival requirements into the design, development, and implementation of electronic information systems; providing training and guidance to personnel with records management responsibilities; developing records schedules for records and obtaining NARA approval; and conducting evaluations to measure the effectiveness of records management programs and practices and ensure they comply with NARA regulations.

Protection Requirements—Privacy

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*.[15] 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.[16] It requires agencies to issue system of records notices to notify the public when they 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.

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.[17] A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. Specifically, according to OMB guidance, the purpose of a PIA is 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

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

[16]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).

[17]Sec. 208, Pub. L. No. 107-347.

protections and alternative processes for handling information to mitigate potential privacy risks.[18]

Protection Requirements—Information Security

FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information or information systems, including the development, documentation, and implementation of an agency-wide risk-based information security program.[19] These protections are to be provided for information collected or maintained on behalf of the agency and information systems used or operated by a contractor of an agency or other organization on behalf of an agency.

Compliance Requirements for Schools Receiving Financial Assistance Program Funding

Federal law and Education regulations set forth requirements with which schools participating in financial assistance programs must comply. Education establishes program participation agreements with schools, which are signed on behalf of the Secretary of Education and the school. The execution of the agreement by the school and the Secretary of Education is a prerequisite for the school's initial or continued participation in any financial assistance programs. The agreement outlines general terms and conditions in which schools are required to understand, agree to, and comply with applicable statutes and regulations, including the *Family Educational Rights and Privacy Act of 1974*[20] and its implementing regulations (34 C.F.R. Part 99) and the *Standards for Safeguarding Customer Information* (16 C.F.R. Part 314),

[18]Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

[19]*Federal Information Security Modernization Act of 2014*, Pub. L. No. 113-283, (Dec. 18, 2014); 44 U.S.C. §§ 3551-3558 (FISMA 2014), largely superseded the very similar *Federal Information Security Management Act of 2002* (Title III, Pub. L. No. 107-347, Dec. 17, 2002) (FISMA 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 continue unchanged.

[20]20 U.S.C. § 1232g.

issued by the Federal Trade Commission under the *Gramm-Leach-Bliley Act*.[21] These standards are intended to insure the security, confidentiality, and integrity of customer information.

In particular, the *Gramm-Leach-Bliley Act* established an obligation for financial institutions to protect the security of their customers' information, and required the development of related security standards. This is the basis for the Federal Trade Commission's *Standards for Safeguarding Customer Information*, which applies to schools by virtue of the financial relationships they have with students, donors, and others.

Under the Federal Trade Commission standards, schools must adopt an information security program, develop detailed policies for handling financial data covered by the law (e.g., parents' annual income), and take steps to protect the data. Specifically, schools are to develop, implement, and maintain a comprehensive information security program that includes:

(1) employee(s) designated to coordinate the program;

(2) an assessment of risks to the security, confidentiality, and integrity of customer information;

(3) design, implementation, and testing and monitoring of safeguards to control the risks identified;

(4) evaluation and adjustment of the program in light of testing and monitoring; and

(5) oversight of service providers, including reasonable steps to select and retain providers capable of maintaining appropriate safeguards and requiring the implementation of such safeguards by contract.

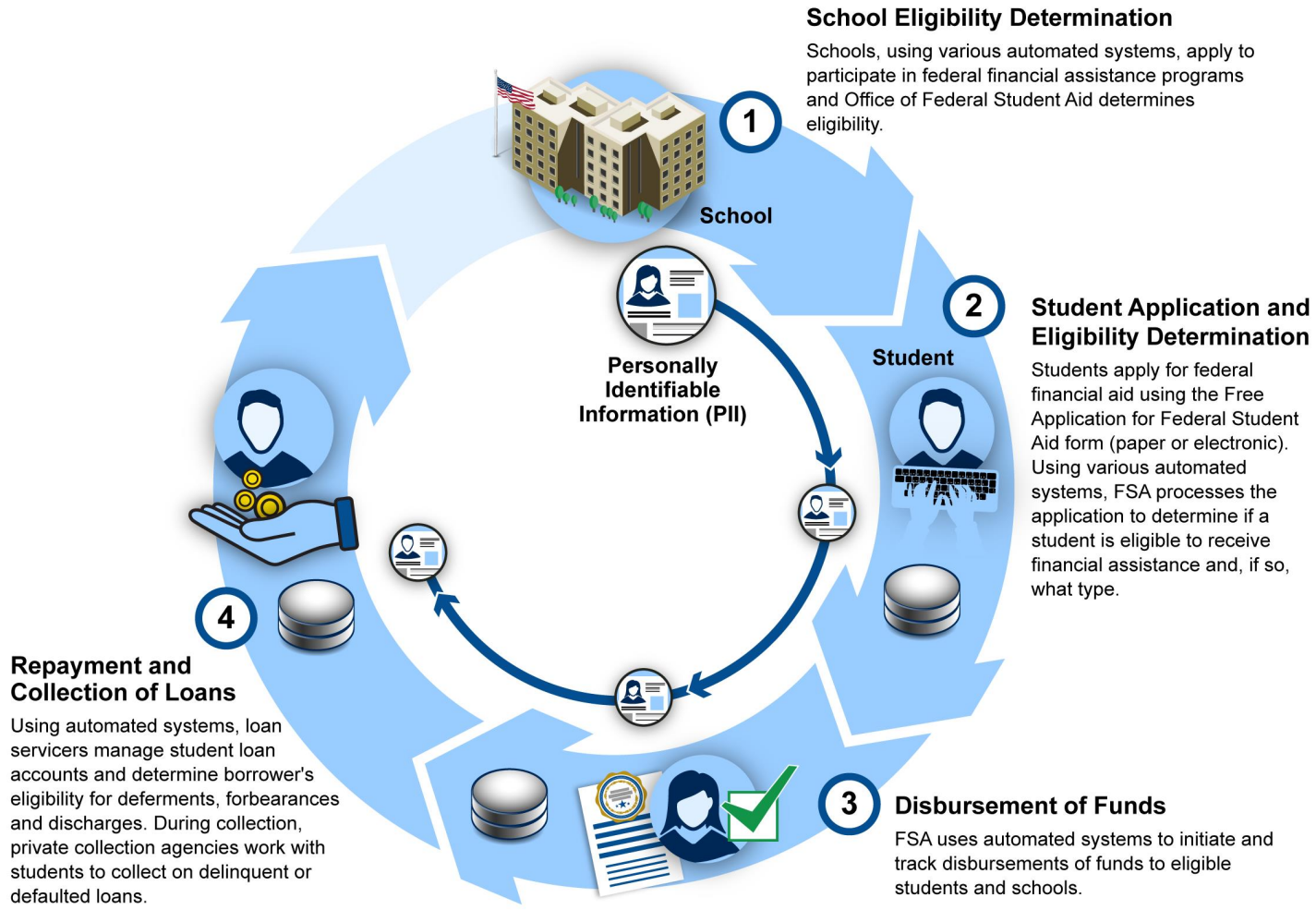
[21]Sections 501-502, Title V, subtitle A, Pub.L. No. 106-102 (Nov. 12, 1999); 15 U.S.C. §§ 6801-6802.

FSA and Schools Use Personal Information to Support Financial Assistance Application, Disbursement, and Repayment Activities

FSA and schools use a variety of personal information, including PII collected from students, their families, and others, to support the federal financial assistance process. This process involves multiple participants, and activities conducted in four phases: (1) school eligibility determination, (2) student application and eligibility determination, (3) disbursement of funds, and (4) 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, including federal agencies such as the Social Security Administration and the Department of Justice, to assist FSA and schools in determining aid eligibility, type and amount of aid a student is eligible to receive, and distribution and repayment of loans.

Figure 1 provides a simplified overview of FSA's financial assistance process and the following sections further describe the process. In addition, appendix II provides a listing of the automated systems used throughout all four phases of the financial assistance process and the personal information collected and used.

Figure 1: Simplified Overview of the Financial Assistance Process of the Office of Federal Student Aid (FSA)



Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

Phase 1: School Eligibility Determination

During this phase, FSA collects information from schools to determine their eligibility to participate in the financial assistance programs.[22] Specifically, to participate in financial assistance programs, schools must be certified by FSA. To receive certification, schools are required to complete an application for approval to participate and submit supporting documentation, which FSA uses to examine the school's institutional eligibility, administrative capability, and financial responsibility. In completing the application, schools are to use FSA's Electronic Application for Approval to Participate system. This system collects, among other things, information regarding a school's accreditation status to provide postsecondary education, the type of school structure (e.g., public, private, nonprofit), and the educational programs the school offers.

Schools also use the Electronic Application for Approval to Participate system to elect to participate in one or more campus-based programs, such as the Federal Perkins Loan Program, the Federal Supplemental Educational Opportunity Grant Program, and Federal Work-Study. If a school elects to participate in campus-based programs, it must complete and submit a Fiscal Operations Report and Application to Participate form through FSA's eCampus-Based system.[23] FSA uses this information to determine the amount of funds a school may receive for each campus-based program.

[22]FSA's information collections are conducted with forms that have been approved by OMB through the information collection review process, as required by the *Paperwork Reduction Act*, 44 U.S.C. §§ 3506(c), 3507, and 3508. The Free Application for Federal Student Aid is the primary form used by FSA to collect student's information throughout the federal student financial aid process.

[23]The eCampus-Based system collects PII about the school's designated user of the system, such as the user's name, address, telephone number, e-mail address, along with the school's financial information.

Program Participation Agreement

To participate in FSA programs, a school must have a current Program Participation Agreement. Within the agreement, the school agrees to comply with the laws, regulations, and policies governing FSA programs. It contains critical information such as the effective date of a school's approval, the date by which the school must reapply for participation, and the date the approval expires, the agreement lists the FSA programs, such as Pell Grant and/or Federal Work-Study, in which the school is eligible to participate.

Source: Department of Education, Office of Federal Student Aid documentation. | GAO-18-121

As part of the school eligibility process, FSA requires schools to electronically submit their compliance audits and audited financial statements via FSA's EZ-Audit system.[24] Nonprofit and public schools are also required by OMB to submit the results of their *Compliance Supplement* audits in writing to the Federal Audit Clearinghouse (details of these audits are discussed later in this report).[25] After the school is certified and enters into a participation agreement with the department, the school uses FSA's Student Aid Internet Gateway Participation Management system[26] to enroll its designated authorized user for electronic access to certain FSA systems, including the Central Processing System (CPS) and the Common Origination and Disbursement (COD) system. After the school enrolls for electronic access, the school's designated user can then access the Student Aid Internet Gateway to securely exchange data, such as student application information or loan and grant data, electronically with FSA systems, including CPS, COD, and the National Student Loan Data System, among others.[27]

In addition, FSA uses other systems to manage its participation process. For example, FSA's Postsecondary Education Participants System, stores information collected during the school eligibility process and is the management information system of all organizations that participate in administering student financial aid. Specifically, the system maintains eligibility, certification, demographic, financial, review, audit, and default

[24]The EZ-Audit system collects PII about the school's designated user of the system, such as the user's name, telephone number, e-mail address, along with the school's financial information.

[25]The Federal Audit Clearinghouse operates on the OMB's behalf and its primary purposes are to distribute single audit reporting packages to federal agencies and support OMB oversight and assessment of federal award audit requirements.

[26]The Student Aid Internet Gateway Participation Management system collects PII about the school's designated user of the system, such as the user's name, address, telephone number, date of birth, Social Security number, and mother's maiden name.

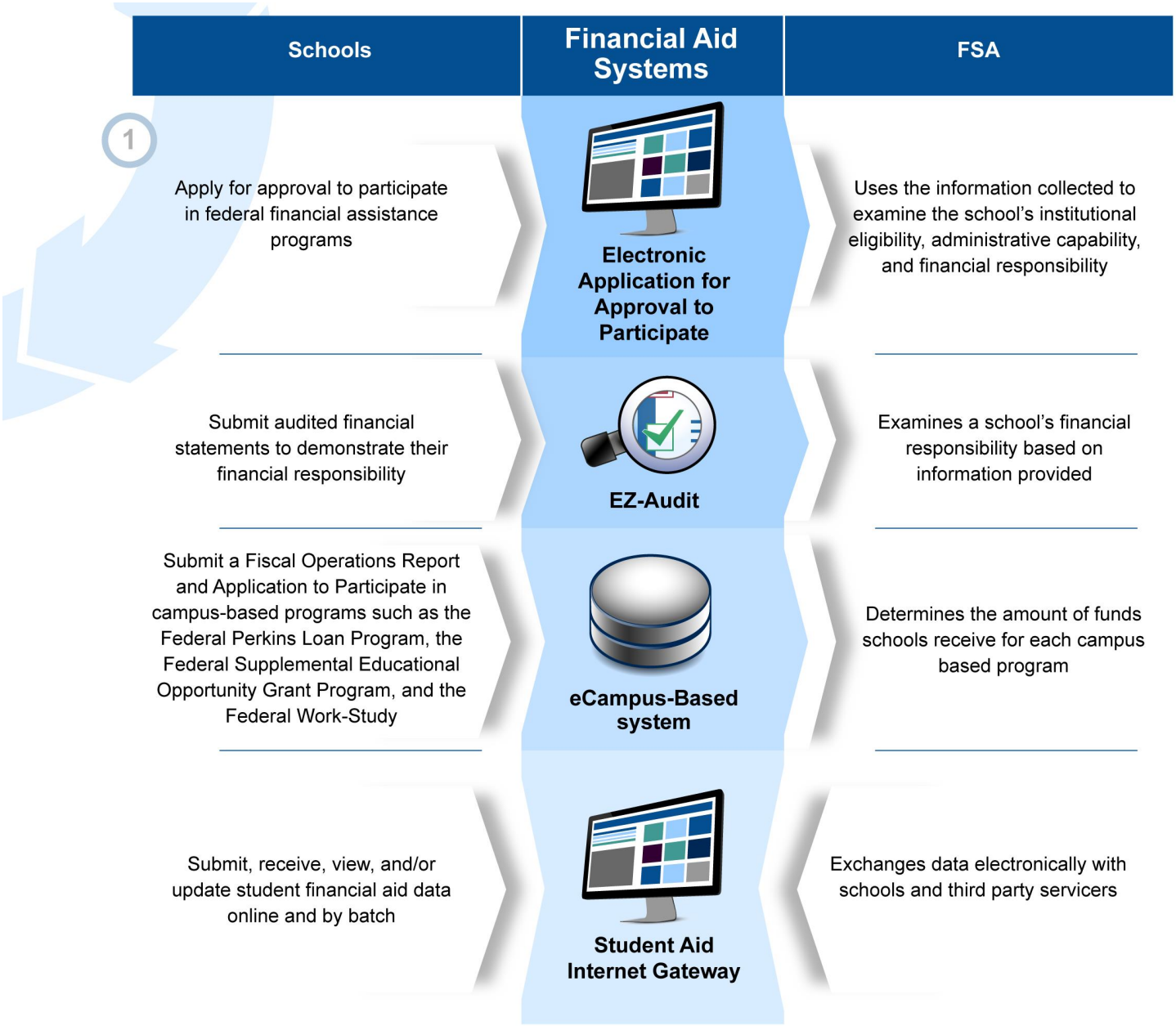
[27]The National Student Loan Data System is FSA's central database for student financial aid. It contains student-level data received from schools, the Direct Loan Program, the Pell Grant Program, and other Education programs and offices. It also provides a centralized, integrated view of federal student aid loans and Pell Grants and tracks them through their life cycle.

rate data about schools, lenders, and guarantors participating in federal financial assistance programs.[28]

Figure 2 provides an overview of FSA's process for determining school eligibility.

[28]According to FSA officials, a new system, the Integrated Partner Management system, will replace the following systems: the Electronic Application for Approval to Participate, EZ-Audit, and the Postsecondary Education Participants System. The Integrated Partner Management system, originally scheduled to be in place by September 2017, was delayed as a result of user acceptance testing. FSA has not determined a new deployment date.

Figure 2: Overview of the School Eligibility Determination Process of the Office of Federal Student Aid (FSA)



Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

Phase 2: Student Application and Eligibility Determination

The second phase of the process involves students applying for federal student aid, the processing of student applications, and the determination of what types and amounts of aid they qualify for. To be considered for federal student aid, a student must apply and complete a Free Application for Student Aid either by telephone, by using a paper form, or online. To submit the application online, the student is required to create an FSA username to electronically sign and send the form to FSA.

The application collects information about the student and/or parent that includes, but is not limited to the following:

- **Student demographics**—name, address, Social Security number, telephone number, e-mail address, marital status, driver's license number.
- **Student eligibility**—citizenship status, dependency status, high school completion status, Selective Service System 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, e-mail address, and marital status.
- **Parent finances**—tax return filing status, adjusted gross income, tax exemptions, and asset information.

After the student submits the student aid application, it is then processed by FSA's CPS. This system stores and uses the information collected from the application, such as the student's demographic and eligibility information, to determine whether the student is eligible to receive federal student aid. The system also performs a data check against FSA's National Student Loan Data System and those maintained by other federal agencies, including the Departments of Defense, Homeland Security, Justice, and Veterans Affairs, the Social Security Administration, and the Selective Service System registration database. During the data checks, CPS validates students' and parents' Social Security numbers and verifies citizenship status through a data match with the Social Security Administration. CPS also verifies that the name and birth date

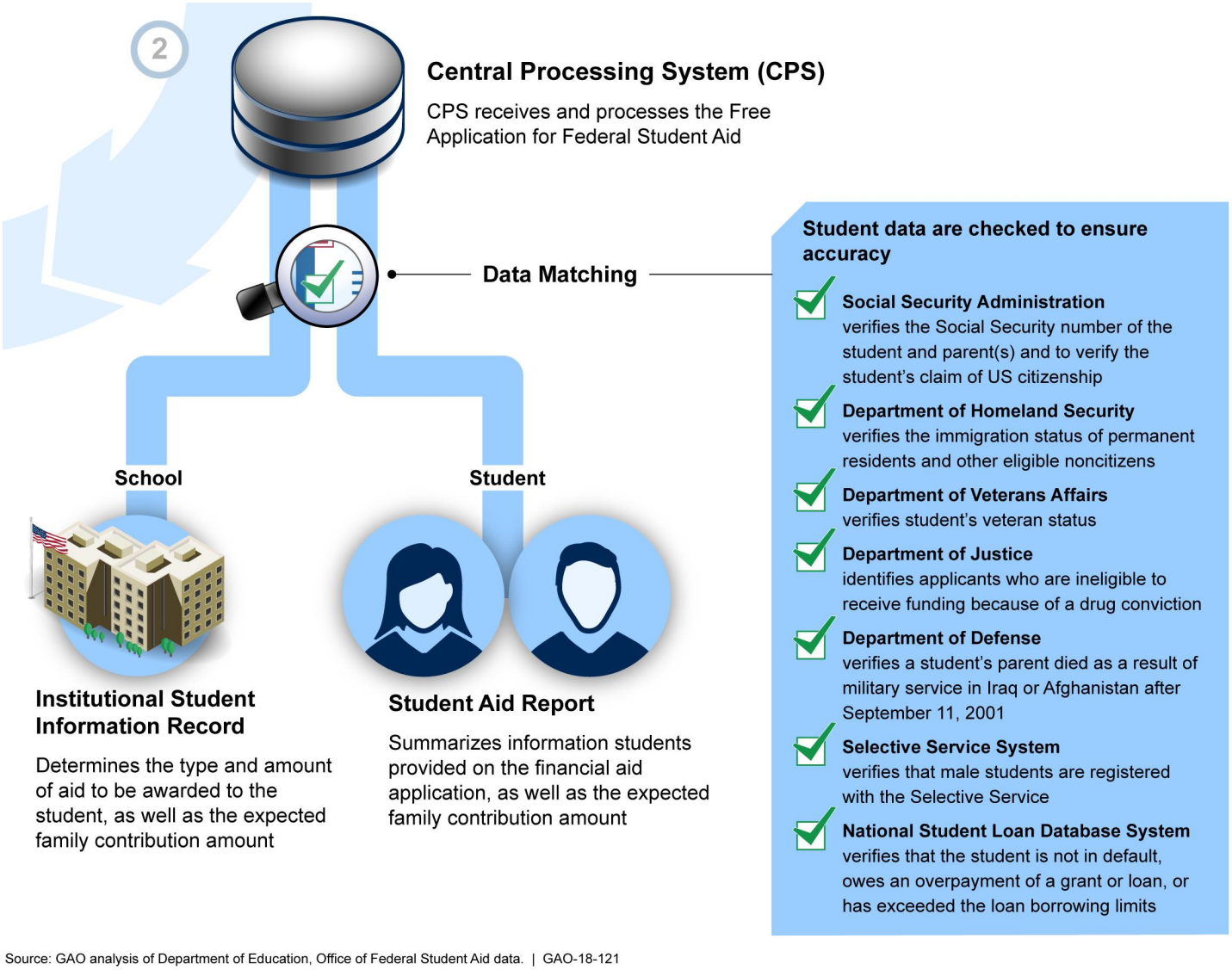
associated with the Social Security number match the name and birth date on the application.

To ensure the accuracy of the application data, CPS also checks the application for inconsistencies and mistakes. For example, if a dependent student reported the parents' marital status as married but reported the household size as two, edit checks in the system would flag the inconsistency. In addition, CPS accesses the Postsecondary Education Participants System to confirm that the designated schools listed on a student's financial aid application are eligible to participate in financial assistance programs.

Further, CPS uses the PII provided on the application to calculate the expected family contribution amount, which schools will use to help determine the amount of the student aid award. The expected family contribution is a measure of how much the student and his or her family can be expected to contribute to the cost of the student's education for the year. The contribution is calculated according to a formula specified in the *Higher Education Act*. The expected family contribution formula uses several variables from the financial aid application, including income, assets, the number of persons in the household, and the number of students in the household attending college for the award year.

After CPS completes its processing of the application, CPS produces two documents that notify schools and the student, respectively, of the expected family contribution calculation results. One document is the Institutional Student Information Record, made available to the designated schools listed on the student's application. This document includes financial aid application data and the expected family contribution amount. Schools then use the information to determine the types and amount of aid to be awarded and notify the student with an award letter. The other document produced is the Student Aid Report. This report, which is mailed or made available online to the student, summarizes the information provided by the student on the application, as well as the expected family contribution amount; the results of the eligibility database matches; and information about any inconsistencies identified during processing. Figure 3 is a depiction of the student eligibility determination process—the second phase of the student financial aid process.

Figure 3: Student Financial Aid Application and Eligibility Determination



Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

Phase 3: Disbursement of Funds

The third phase of the process involves FSA disbursing funds to schools. When federal student aid funds—such as grants, loans, and work-study—are disbursed to schools, those institutions hold the funds in trust for the

student.[29] Schools typically apply the money to a student's school account to cover such expenditures as tuition, room, and board. In this phase, FSA uses the COD system to interact with other FSA and Education systems. FSA also uses COD to initiate and track disbursement of funds to eligible students and schools.

To facilitate the disbursement process, COD receives, processes, and stores personal information, including students' names, Social Security numbers, current addresses, dates and places of birth, telephone numbers, and funding amounts. The system verifies that the information sent by the school is correct and complete. To do so, for example, the system verifies students' eligibility information in CPS, including the expected family contribution amount, using the personal information originally provided on the student financial aid application.

In addition to using CPS for verification, COD sends to, and receives data from, the National Student Loan Data System to update students' grant and loan disbursement information. Further, COD uses students' personal information as a unique identifier to initiate loans, account for awarded loans and grants, and reconcile the financial aid amounts that schools receive to the amounts that the schools disburse to eligible students. After COD validates and verifies student and school information, these data are maintained in the system and also are used to create disbursement data that drive funding transactions.[30]

Next, in order to provide funds to schools, Education's Grant Management system is used to validate that the school is eligible to receive funding. The system then provides this data to both the department's and FSA's financial management systems. Specifically, Education's Financial Management Support System disburses the funds

[29]Before a school can originate a loan with, and receive funds from FSA, the student that is to receive the loan as part of their award package must complete entrance counseling and sign a master promissory note through FSA's studentloans.gov website. Once loan counseling is completed, the school then receives a confirmation in their Student Aid Internet Gateway system mailbox. As previously discussed, the Student Aid Internet Gateway allows schools to exchange data electronically with FSA.

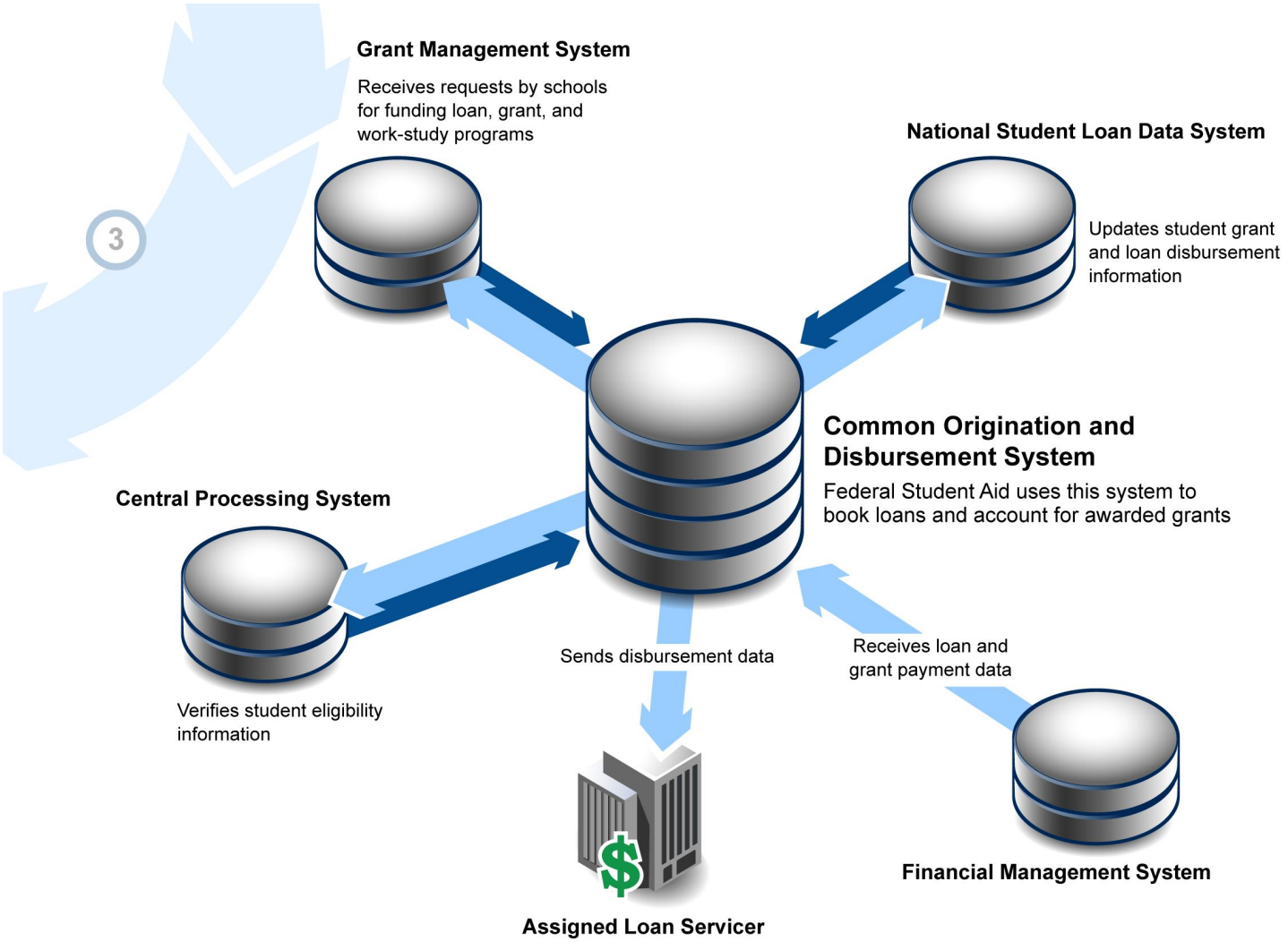
[30]In response to our survey, an estimated 63 percent of schools that participate in federal financial assistance programs collect and use PII, such as financial information, school-related information, and student/parent employment information, to support the disbursement of federal financial aid, including loans, grants, and federal work-study.

to schools, while FSA's Financial Management System sends the loan and grant payment data to the COD system.[31]

For loan disbursements, COD sends the loan data, which include the student's personal information, to the student's assigned loan servicer. The loan servicer records the borrower's loan and sends summarized financial transactions to FSA's Financial Management System. This system further summarizes the loan booking financial transactions and sends them to Education's Financial Management Support System. Figure 4 depicts the exchange of information between the systems involved in the third phase of the financial aid process: disbursement of funds.

[31]Funds are disbursed by Education's Financial Management Support System, through the Department of the Treasury, to the schools.

Figure 4: Information Exchange Between Key Office of Federal Student Aid Systems Involved in the Disbursement Process of Student Financial Assistance Program Funds



Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

Phase 4: Repayment and Collection of Loans

The final phase is repayment and collection of loans. After the disbursement of funds, students' collected personal information is stored on FSA systems and used by the agency to share among its financial partners, including loan servicers, guaranty agencies, and private collection agencies that work in support of Education.

Before loan repayment begins, students notify Education of their choice of an initial repayment plan. Loan servicers, operating on behalf of FSA, store and use the students' information to provide assistance with managing the loans, locating borrowers in cases of invalid addresses and/or telephone numbers, and for determining borrower eligibility for entitlements such as deferments, forbearances, and discharges.[32] For example, students can request deferments because of unemployment, temporary total disability, economic hardship, and military service, among other reasons. When requesting such entitlements, students provide their personal information; and for total temporary disability deferment requests, private medical information.

Loan servicers also share students' information with FSA and other entities. For example, loan servicers share students' information with internal FSA systems, such as the National Student Loan Data System, to report updates to payment information, loan status, and contact information. Further, students' information is shared with external entities, such as consumer reporting agencies, to report credit history and to resolve credit report disputes.

In addition, with regard to the Federal Family Education Loan program, private lenders made federal loans to students, and guaranty agencies insured these funds, which were, in turn, reinsured by the federal government. To manage this process, guaranty agencies use their own automated systems that communicate with internal FSA systems. As noted previously, this program ceased issuing new loans in July 2010. However, FSA continues to administer the program, while lenders and guaranty agencies continue to service and collect outstanding loans in the Federal Family Education Loan program portfolio.

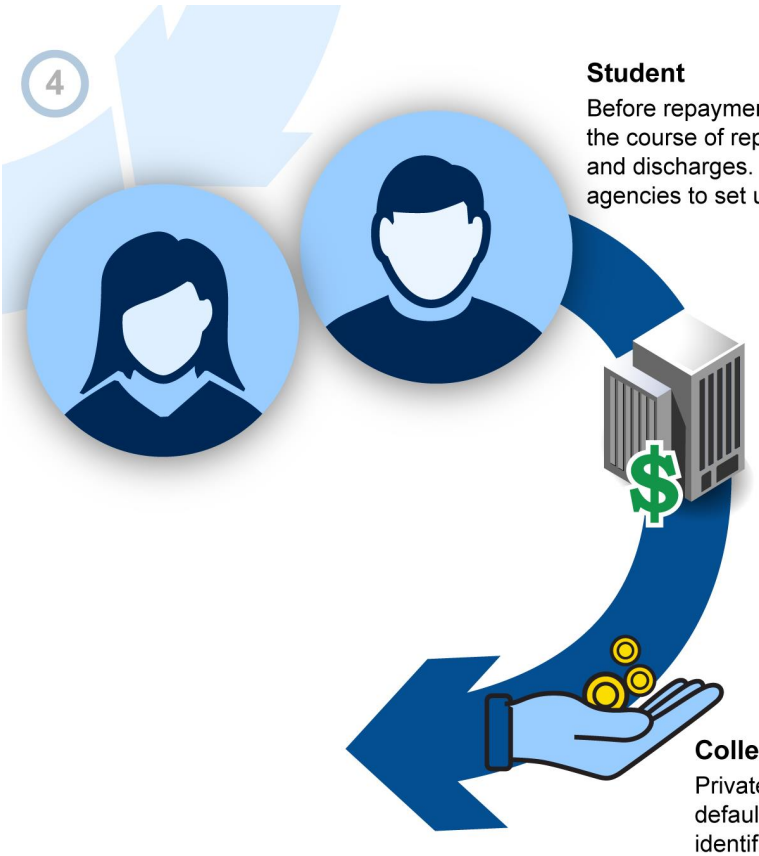
For loan defaults, the Debt Management and Collection System vendor and private collection agencies work with students to encourage full loan repayment, while ensuring that defaulted borrowers are aware of both the consequences of their failure to repay and the options available to help

[32]A deferment is a postponement of payment on a loan that is allowed under certain conditions and during which interest does not accrue on direct subsidized loans, Subsidized Federal Stafford Loans, and Federal Perkins Loans. Forbearance is a period during which monthly loan payments are temporarily suspended or reduced. A discharge releases the borrower from the obligation to repay his or her loan.

them get out of default.[33] The Debt Management and Collection System vendor and private collection agency systems collect, store, and update borrowers' information to provide account management, repayment servicing, and payment collection, among other things. In addition, the information that is collected, stored, and updated by private collection agency systems is shared with FSA, the Department of the Treasury, and national consumer credit agencies, among others. This information is used to locate borrowers and enable recovery and/or resolution of defaulted student loans. For example, the Department of the Treasury uses the borrower's information to withhold federal payments such as federal income tax refunds, Social Security payments, and other federal payments to collect on defaulted federal student loans. Figure 5 depicts the repayment process in the fourth phase of the financial aid process: repayment and collection of funds.

[33]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.

Figure 5: Repayment Process for Student Financial Assistance Funds



Student

Before repayment begins, students choose an initial repayment plan. During the course of repayment, students can also apply for deferments, forbearances, and discharges. During collection, students can work with private collection agencies to set up payment collection in cases of default.

Repayment

Loan servicers use various automated systems to manage student loans and determine borrower eligibility for deferments, forbearances, and discharges using the borrower's personally identifiable information.

Using automated systems, guaranty agencies insured Federal Family Education Loan program funds that private lenders made to students.

Collection

Private collection agencies work with borrowers whose loans are in default. Private collection agencies share the borrower's personally identifiable information with external entities such as the Department of Treasury and national consumer credit agencies to locate borrowers and to enable recovery and/or resolution of defaulted loans.

Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

During all phases of the financial assistance process, FSA's ombudsman case tracking system can be used by any student who chooses to file a complaint.[34] This can be done anonymously, using the borrower's information or using their FSA username and password.

[34]The Ombudsman Case Tracking System/Enterprise Complaint System, as a collective system, manages the information and activities associated with the resolution of customer issues involving disbursement and servicing of federal student loans. It also provides students and borrowers with the means to file complaints and provide feedback about federal student loan lenders, servicers, collection agencies, and schools.

To process the complaint, FSA uses the student's information, such as date of birth and Social Security number, to review the student's or borrower's financial aid and disbursement history in order to address the complaint or dispute. FSA's Integrated Student Experience system[35] collects this information for the ombudsman and transmits it to the Ombudsman Case Tracking System/Enterprise Complaint System to process the complaint.

Policies for Managing and Protecting Student Aid Records Largely Reflect Federal Requirements, but Weaknesses Exist in FSA's Procedures

Education has established policies and procedures for managing records that address requirements established in the *Federal Records Act* and NARA regulations. These department-wide policies and procedures establish records management responsibilities for Principal Offices within the department, such as FSA. Accordingly, FSA has established procedures for addressing these requirements, including those for identifying and scheduling its records, archiving and destroying certain temporary records, training personnel on records management responsibilities, and conducting a self-assessment of its records program. However, weaknesses in key FSA procedures reduce assurance that student aid information, including personal information, is being managed in accordance with Education policies and requirements.

With respect to the protection of data, the department has established policies and guidance for the protection of PII and the security of information systems that reflect requirements found in federal laws and guidance. However, while FSA established procedures for meeting key privacy and security requirements, its method used to assess privacy risks and mitigation steps did not consistently address key elements called for by federal guidance. Also, FSA's information security policies have not always been regularly updated to ensure they reflect current practices and requirements.

[35]The Integrated Student Experience system collects and transmits information for the FSA ombudsman via the FSA ombudsman online form, among other things.

FSA Has Established Policies for Carrying Out Records Management Responsibilities, but Shortcomings in Its Procedures May Hinder Their Effectiveness

As previously mentioned, the *Federal Records Act* requires federal agencies to establish and maintain an active, continuing program for the economical and efficient management of the records of the agency.[36] To implement the provisions of the act, NARA issued regulations with specific requirements for agency records management programs.[37]

Consistent with the *Federal Records Act* and NARA regulations, Education has developed and issued policies and procedures for managing records in its possession.[38] For example, the department's directive on its Records and Information Management Program outlines records management responsibilities and requirements. These include, among others, requirements for Principal Offices to ensure that their records are organized, scheduled, and archived or disposed of as appropriate.

FSA has developed procedures and tools for managing federal student aid records. These procedures include records schedules documenting the retention and disposition of federal student aid records, a file plan for organizing paper records and certain electronic files, procedures for the transfer and final disposition of paper-based records, a process for records management training, and a process for conducting a triennial assessment of its records management program.

However, shortcomings exist in key FSA procedures for managing its records. Specifically, FSA has not fully established procedures for managing electronic records through their final disposition, and it has not ensured regular records management training for employees, or carried out a required self-assessment of its records management program.

[36]44 U.S.C. § 3102.

[37]36 C.F.R. Part 1220.

[38]These include two Education directives: *Records and Information Management Program*, OM 6-103 (May 2016), and *Records Retention and Disposition Schedules*, OM 6-106 (November 2007), as well as other guidance such as guidance such as the *Records Liaison Officers File Plan Manual* (issued by the Records and Documents Management Division of the Office of the Chief Privacy Officer).

Table 3 summarizes the extent to which FSA established procedures for meeting its records management requirements. Details of our assessment are discussed in the paragraphs following the table.

Table 3: Assessment of the Office of Federal Student Aid Procedures for Meeting Records Management Responsibilities Established by Education

Requirement	Procedure established
Identify program-specific records and ensure they are covered by a National Archives and Records Administration (NARA) disposition schedule	Fully
Complete a file plan to guide how files are managed and organized	Fully
Ensure that records are transferred into storage or promptly destroyed according to NARA-approved records disposition schedules and that records management requirements are incorporated into electronic information systems	Partially
Ensure that personnel with records management responsibilities receive adequate training	Partially
Conduct internal assessment of the records management program, including an in-depth review every 3 years	Partially

Legend: "Fully" established = FSA provided evidence that the agency had addressed all aspects of a requirement; "partially" established = FSA provided evidence that the agency addressed some but not all aspects of a requirement.

Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

FSA Established Procedures for Ensuring Program-Specific Records Are Covered by a Disposition Schedule

According to Education's records management directive, Principal Offices within the department, in conjunction with Education's records officer, are responsible for ensuring that their records are covered by a NARA-approved records schedule.[39] To determine the appropriate retention period for each type of record, Education policy directs Principal Offices to consider whether the retention period is adequate to meet the business needs for the records, fiscal needs, and legal requirements.

[39]According to Education policy, after Principal Offices prepare schedules for their records, the schedules are reviewed within the department and then submitted to NARA for approval. After a review process, which may include questions from NARA, site visits, and requests for additional information, the records officer notifies originating offices whether their schedules have been approved.

FSA has established procedures for ensuring that program-specific records are covered by NARA-approved schedules. Specifically, FSA has developed and issued 10 program-specific records schedules that have been approved by NARA.[40] These schedules cover a variety of records created during the student aid process. Among others, the records include information provided by students when applying for aid and records of aid disbursed.

The schedules describe the records and provide disposition instructions, implementation guidance, and restrictions, such as those imposed by the *Privacy Act of 1974*. The records have been classified by FSA as temporary, and their retention periods range from 2 years to 75 years, with most having a retention period of 15 years after cutoff.[41]

Table 4 describes the record types included in FSA's schedules related to the federal student aid process and their associated retention and disposition information.

Table 4: Types of Records and Their Disposition and Retention Periods as Identified by Federal Student Aid Records' Schedules

	Record type	Disposition	Retention period
Phase 1: School application and eligibility determination	Information provided by institutions to participate in Title IV programs,[a] including data on eligibility, administrative capacity, and financial responsibility; financial statements and compliance audits; and application forms submitted by schools to participate	Temporary	30 years after cutoff at the end of the fiscal year when final action is completed
	Information provided by schools, among other entities, to gain electronic access to Office of Federal Student Aid (FSA) systems, which includes personally identifiable information from school users	Temporary	6 years after user account is terminated or when no longer needed for other specified purposes
	School user account information for access to FSA systems	Temporary	6 years after 2-year archival period
Phase 2: Student application and eligibility determination	Information from students, parents, and borrowers to establish user credentials for access to FSA systems	Temporary	2 years after annual cutoff

[40]Several of these schedules cover one or more types of records.

[41]According to the National Archives and Records Administration, cutoffs are convenient points within a filing plan/system (end of a letter of the alphabet, end of year or month, etc.) at which files are separated for purposes of storage and/or disposition.

	Record type	Disposition	Retention period
	Student application records, including data from the Free Application for Federal Student Aid	Temporary	15 years after final repayment or audit of obligation
	Data related to processing financial aid and determining Title IV eligibility; includes data from the Free Application for Federal Student Aid matched with other government systems	Temporary	15 years after final repayment or audit of obligation
Phase 3: Disbursement of funds	Loan origination and disbursement records (e.g., master promissory notes, loan application and disbursement information)	Temporary	Master promissory notes are to be destroyed 5 years after payoff for paid-off loans; 75 years after issuance for defaulted loans Other loan origination and disbursement records are to be destroyed/deleted 15 years after final repayment or audit
	Information about loans and grants awarded, including student name, loan period, type of loan, repayment cycle, etc.	Temporary	15 years after annual cutoff[b], which occurs when account is paid in full
	Student loan data related to financial transactions for loans, grants, campus-based programs	Temporary	15 years after cutoff[b]
Phase 4: Repayment of funds	Loan servicing, consolidation, and collections records, including data on individual borrowers	Temporary	15 years after cutoff[b], which occurs annually upon repayment or discharge of loan
	Records generated to calculate school cohort default rates or support challenges, adjustments, and appeals by schools (may include information on individual borrowers)	Temporary	10 years after annual cutoff[b] following review for fiscal year
	Ombudsman records documenting efforts to address and resolve borrower complaints related to student loans	Temporary	10 years after cutoff[b] on close of case or final determination

Source: GAO analysis of Department of Education, Office of Federal Student Aid records schedules. GAO-18-121

[a]Title IV programs are student assistance programs authorized under Title IV of the *Higher Education Act;* FSA is responsible for administering and overseeing Title IV programs.

[b]According to the National Archives and Records Administration, cutoffs are convenient points within a filing plan/system (end of a letter of the alphabet, end of year or month, etc.) at which files are separated for purposes of storage and/or disposition.

FSA is awaiting approval of two additional schedules for program-specific records. Specifically, NARA has not yet approved FSA's schedules for the records related to the Person Authentication Service and the Health Education Assistance Loan Online Processing system. The Person Authentication Service, which replaced the personal identification number registration system in 2015, generates login credentials allowing users to access systems in order to obtain information about their personal records. The Health Education Assistance Loan Online Processing

system is used to process claims for borrowers who default.[42] Both systems collect personal information from users. In July 2017, FSA records management officials told us that both schedules had been submitted to NARA for approval.

FSA Established a File Plan That Enables It to Organize and Manage Paper and Certain Electronic Records

Education guidance calls for each Principal Office to complete a file plan, which is a guide to how records are managed. The file plan is to consist of a list of: (1) records, in all formats (e.g., paper and electronic) being maintained in an individual office, central file area, or electronic platform, such as a shared drive; (2) the location of the records; (3) the name of the person responsible for them; and (4) the retention period and final disposition of the records (i.e., whether they are temporary or permanent).

FSA has established a file plan in accordance with Education's requirements. The plan specifies categories, record series and descriptions, disposal instructions, and the locations of the records, among other elements. Record categories include various types of administrative records, as well as both paper and electronic files documenting student participation in federal financial assistance programs.

FSA Established Procedures for Transferring and Disposing of Physical Records, but Its Guidance for Electronic Information Systems Does Not Address the Disposal of Electronic Data Files Containing Student Records

Education policy requires Principal Offices to ensure that records are transferred into off-site storage or promptly destroyed according to NARA-approved records disposition schedules. Accordingly, FSA has a procedure for transferring and disposing of physical records. Specifically, the agency's guidance outlines steps for packing, labeling, and shipping records, both temporary and permanent, to federal records centers for storage and for disposal notification.

[42]The Health Education Assistance Loan Program ended on September 30, 1998, but Education retains responsibility for handling loan repayments.

According to FSA records management officials, the agency uses offsite archival storage that is provided by a departmental interagency agreement with NARA federal records centers. In this regard, records are indexed, boxed, and stored in the applicable federal records centers that align with the department field offices. The archival boxes are held at the records center until the end of the retention period, as specified in the records schedule. At that time, NARA implements a vetting process, organized through the department's records officer in unison with FSA, which verifies that the records are or are not needed to fulfill any business or legal requirements. Once cleared by Education's Office of General Counsel and the responsible program office, the department records officer receives a signed destruction notice from FSA that authorizes NARA to proceed with the destruction process as prescribed in the disposition authority.

The department's policy on records and information management also requires its Principal Offices to ensure that electronic information systems containing records have records management processes and requirements incorporated into their design and operations. These include requirements for records creation and storage, and the deletion of temporary records in accordance with the relevant disposition schedule.

However, FSA did not provide evidence of a procedure for the destruction of electronic data files in the electronic information systems that support much of the student aid process. Such systems collect, store, and process many records containing student information, and FSA has established disposition and retention periods for these records, as discussed previously.

According to FSA officials, records management requirements for these systems are addressed through FSA's Lifecycle Management Methodology, which provides a governance model for information technology projects throughout their life cycle. This methodology states that all of FSA's information system projects are expected to tailor their approach to adhere to the Lifecycle Management Methodology, according to the project's chosen system development life cycle. The methodology and its associated guidance include requirements related to managing records in FSA's systems. This includes requirements for developing and reviewing:

- retention schedules for the data in the electronic systems;

- configuration management templates that include data management requirements, such as data distribution;
- system of records notices; and
- system disposal plans that document the data that need to be preserved or disposed of when a system is retired.

Nevertheless, while the methodology includes a requirement for the development of records retention and disposition schedules for data contained in a system, it does not discuss how the records are to be disposed of in accordance with their schedules. Specifically, the methodology includes guidance for the archiving or disposal of data when a system itself is decommissioned, but it does not describe a process for identifying and approving the archiving or disposal of records once they have reached the end of their retention period as defined by their associated records schedules. Further, the methodology does not address the deletion of records in accordance with the relevant disposition schedule.

As noted above, student aid records, including those contained in electronic information systems, have specified retention periods. The disposition of such records should occur in accordance with their schedules. However, FSA's Lifecycle Management Methodology addresses disposal activities when a system is retired, but not when records reach the end of their retention period. Without including a procedure for disposing of records contained in electronic systems, FSA may retain data files containing student records longer than needed.

FSA Staff Did Not Always Receive Annual Records Management Training

NARA and OMB require federal agencies to establish a method to inform all employees of their records management responsibilities and develop suitable training for appropriate staff.[43] In conjunction with this requirement, Education policy assigns its Principal Offices the responsibility for ensuring that personnel with records management responsibilities receive appropriate training.

[43]Office of Management and Budget and National Archives and Records Administration, *Memorandum for the Heads of Executive Departments and Agencies: Managing Government Records Directive*, M-12-18 (Washington, D.C.: Aug. 24, 2012).

FSA has taken steps that partially address this requirement. Specifically, it developed training slides to inform its employees of records management responsibilities. The slides discuss topics such as employee responsibilities, records definitions, the establishment of file plans, and disposition activities; they also include references to the department's records management policy.

Although FSA officials stated that records management training is to be completed annually, according to the officials, the department did not deploy organization-wide mandatory all-employee/all-contractor records management training in 2016. The officials stated that employees will be required to take updated records management training in 2017, although they had not established a date for when this is to occur. Until FSA ensures that its employees receive records management training at least annually, FSA and Education have less assurance that employees are aware of their responsibilities and that federal student aid records are being effectively managed.

FSA Did Not Conduct a Triennial Assessment of Its Records Management Program

NARA requires agencies to conduct formal evaluations of their records management programs. Consistent with this requirement, Education policy requires Principal Offices to conduct internal evaluations of their records management programs to certify that they are operating in compliance with NARA and departmental policies and procedures. This includes conducting an in-depth review of the programs every 3 years, in conjunction with the department's records officer. This review is to consist of, among other things, records sampling, record inventories, records schedule updates, and personalized training.

As of July 2017, FSA had not conducted the triennial self-assessment since 2013. The 2013 assessment looked at whether: randomly selected records were labeled and stored properly; records were reflected in the file plan; records in electronic information systems were scheduled; and staff had received training, among other things. According to the results of the assessment, the agency's overall compliance score was 76 percent, which was determined by the rate of compliance with these requirements within FSA's several component offices.

Examples of the deficiencies identified during FSA's self-assessment were records not being stored properly, a need for the file plan to be updated, and a need for more employee training. FSA provided an e-mail

from Education records officials stating that, as of February 2016, corrective actions for the deficiencies found during the 2013 assessment had been implemented.

However, FSA and Education records management officials told us that the department did not have a sufficient number of staff to complete a subsequent self-assessment. FSA officials added that they expect to complete an assessment in calendar year 2017 although they did not provide any documented plans for doing so. Until FSA conducts the next required self-assessment, shortcomings in its records management processes may go unaddressed, which could lead to student aid records not being managed in accordance with NARA and Education requirements.

Policies for Protecting PII Generally Aligned with Federal Guidance, but Privacy Impact Assessments Did Not Consistently Address Key Elements

As noted previously, protections for PII collected, maintained, and shared by federal agencies are required by federal laws and guidance. These include, among others, policies and processes associated with implementing the *Privacy Act of 1974*, and the privacy provisions of the *E-Government Act of 2002*.

Education has issued a number of polices and established processes related to the protection of PII, including that contained in federal student aid records. Education's policies set forth requirements, responsibilities, procedures, and guidance for protecting the information. For example, the department's directive on implementing the *Privacy Act* describes policies and procedures; roles and responsibilities; and requirements for safeguarding privacy in the collection, maintenance, use, and dissemination of information about individuals and for issuing System of Records Notices.[44] In addition, the directive on implementing the privacy provisions of the *E-Government Act* assigns responsibilities to the Senior

[44]These include department's directive on the *Privacy Act of 1974*, OM 6-104 (August 2006), its directive on the privacy provisions of the *E-Government Act of 2002*, OM 6-108 (September 2016), and its *External Breach Notification Policy and Plan*, OM 6-107. In addition, the department's records and information management policy and directive on developing records schedules address aspects of protecting PII in the context of records management.

Agency Official for Privacy and outlines roles, responsibilities, and requirements for developing PIAs for the department's information systems. Further, the department's external-breach notification plan assigns responsibilities to key officials and outlines procedures that are to be followed upon notice that a breach involving PII, or suspected to involve PII, may have occurred.

The department's privacy-related policies require Principal Offices, such as FSA, to take specific actions to implement privacy requirements. Specifically, Principal Offices are to:

(1) designate a *Privacy Act* coordinator to ensure compliance with the *Privacy Act*; and

(2) ensure that all employees and contractors who design, develop, or maintain a system of records are aware of their responsibilities for protecting information on individuals that is in identifiable form.

These policies also require that

(3) notices be developed that contain specific elements to inform the public about systems of record held by the agency;[45]

(4) visitors to agency websites be informed about what identifiable information may be collected, why it is collected, and how the department will use the information; and

(5) PIAs be developed for electronic information systems and collections that contain PII.

FSA has established procedures for adhering to four of these key department-level privacy requirements. Specifically, it has

- designated a privacy coordinator, identified as the FSA *Freedom of Information Act* Liaison, as well as a privacy advocate, who coordinates with the department privacy officer on breaches, PIAs, and system of records notices.

[45]As required by the *Privacy Act*, agencies must publish in the *Federal Register* notices of systems of records, or system of records notices, that are to contain specific elements about the system of records that is being created.

- put in place a process for ensuring employees are aware of their responsibilities for protecting PII, through administering annual security and privacy awareness training that addresses risks to PII and how it should be protected.
- published system of records notices spanning the various phases of the student aid process that address required elements for informing the public about how personal information is to be maintained, used, and accessed.
- posted its privacy policy on its website and included *Privacy Act* notices on its public-facing web applications for applying for aid, repaying loans, and accessing information about loans to inform users of their rights when being asked to provide PII, and provide descriptions of related privacy protections for that information.

However, FSA did not always adhere to the fifth requirement by ensuring that its PIAs always addressed key elements. Among other things, the assessments must identify what PII is collected, why it is being collected and its intended use, how it will be shared, opportunities for individuals to decline to provide the information or consent to uses of the information, how the information will be secured, and whether a *4* system of records is being created.

Although FSA developed PIAs for its information systems containing PII, the assessments did not always include key elements.[46] Generally speaking, our review of 32 selected PIAs that FSA had conducted determined that the assessments included many key elements, such as what PII was to be collected, why it was being collected, and how it was to be used and shared. However, only 10 of the assessments fully addressed all nine key elements. Table 5 shows the number of PIAs that addressed, partially addressed, or did not address the elements called for by OMB's guidance.

[46]FSA provided a list of 74 active systems in its inventory; of these, it had determined that 60 contained PII. FSA completed PIAs for the systems that it identified as containing PII. We reviewed 32 PIAs created by FSA. Some PIAs covered more than one system. For example, the PIA for private collection agencies covered 30 systems.

Table 5: Number of Office of Federal Student Aid Privacy Impact Assessments That Addressed, Partially Addressed, or Did Not Address Elements Required by OMB Guidance

Required element	Addressed	Partially addressed	Not addressed	Not applicable[a]
What personally identifiable information will be collected	31	0	0	1
What is the purpose of collecting the information	31	0	0	1
How the information will be used	31	0	0	1
How the information will be shared	32	0	0	0
What are the opportunities, if any, for individuals to decline to provide information or consent to particular uses	22	7	1	2
How the information will be secured	18	14	0	0
Whether a system of records is being created	24	2	2	4
What are the risks of collecting, maintaining, and disseminating the information	20	0	11	1
How privacy risks will be mitigated	20	4	7	1

Legend: OMB = Office of Management and Budget.

Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

[a]Some elements were not applicable to particular systems for various reasons. For example, FSA completed a PIA for its Virtual Data Center, but since this hosts other applications that collect personally identifiable information (PII) rather than collecting and storing PII itself, certain elements were deemed not applicable. In addition, two systems do not collect information directly for the public, so the element requiring opportunities to consent to providing the information was deemed not applicable. Finally, in four cases, a system of records notices was not identified because FSA determined that a Privacy Act system of records was not being created.

Specific elements that were not always fully addressed included the following, among others:

- **Opportunities to decline to provide information or consent to particular uses:** PIAs must specify what opportunities individuals have to decline to provide information or to consent to particular uses of the information, and how individuals can grant consent. While 22 of the selected PIAs addressed this element, in 8 cases the PIAs did not discuss opportunities to consent, although 7 of these included some privacy notice information. Without specifying such opportunities, FSA may not be effectively informing individuals of their ability to limit how their PII is collected and used.
- **How information will be secured:** All of the selected PIAs addressed security to some extent; however, 14 of the 32 assessments did not fully address this element. For example, the PIAs did not always state whether or when the system received an authorization to operate—information which is intended to

demonstrate that security controls had been selected, implemented, and tested, as required by OMB guidance.

- **Risks of collecting, maintaining, and disseminating information and associated mitigations:** According to OMB, PIAs are to determine the risks of collecting, maintaining, and disseminating PII and evaluation steps to mitigate these risks. In 20 cases, the PIAs addressed specific privacy risks of collecting, maintaining, and disseminating the information and associated mitigation steps. In 11 cases, however, privacy risks were not addressed, and mitigation steps were either not described or were not linked to specific risks. As a result, less assurance exists that FSA has considered specific privacy risks of collecting, maintaining, and disseminating PII in its systems, and the appropriate steps for mitigating these risks.

In addition, not all of FSA's PIAs were up to date. Department policy states that PIAs are to be reviewed whenever a system change creates new privacy risks and at least every 2 years, and then updated as needed. However, 23 of the 32 PIAs we reviewed had dates more than 2 years in the past, with some dating back 5 years or more.

Department privacy officials acknowledged that the PIAs did not include all required elements. They added that FSA is implementing additional clarification guidance and review steps to ensure that its PIAs are corrected and that the appropriate processes are followed, and that additional end-user training will be provided.

The department provided a revised template for PIAs, dated January 2017. Privacy officials stated that the new template identified additional elements to be addressed, which is intended to ensure that PIAs comprehensively address all OMB requirements. For example, the template requires PIAs to include an assessment of privacy risks and their mitigations, as well as information about the system's authorization to operate.

According to FSA officials, the template is being applied prospectively, so it will be used for all new systems, as well as for all existing systems that need to be updated. However, the officials did not identify specific plans to update the existing PIAs, several of which do not appear to have been updated in several years, as noted earlier. Ensuring that PIAs are up to date and address key elements, as specified by the updated department guidance, will provide additional transparency regarding the risks associated with collecting PII from students and greater assurance that they have been adequately mitigated.

FSA Has Established Policies and Procedures for Protecting Its Information and Systems, but Not All of Them Are Up to Date and Weaknesses Exist in Implementation

FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations and assets of the agency. This is to include those systems provided or managed by another agency, contractor, or other source. To help implement these requirements, the National Institute of Standards and Technology (NIST) provides guidance to federal agencies, such as its guidance on security and privacy controls for federal information systems and organizations.

NIST also states that information security policy is an essential component of information security governance. An agency's information security policy should address the fundamentals of the information security governance structure, including information security roles and responsibilities; a statement of the baseline of security controls; and rules of behavior that agency users are expected to follow. Also, according to NIST, supporting guidance and procedures on how to effectively implement specific controls across the enterprise should be developed to augment an agency's security policy. Further, agencies should also ensure that their information security policy is sufficiently current to accommodate the information security environment and agency mission and operational requirements.

FSA has established information security policies and procedures for implementing security controls called for by federal guidance. These policies and procedures, which include policies promulgated by Education that apply to FSA, address the security control areas outlined in the NIST guidance. These policies and procedures address topics such as controlling access to agency systems, identifying and authenticating users, and conducting risk assessments.

Nevertheless, in some cases, both FSA and department-level Education policies and procedures were not up to date. FSA's guidance on creating and updating technology office security and privacy documentation states that all standards, procedures, guidance, handbooks, and templates are to be reviewed at least annually by document owners and the reviews are to be noted in the document's revision history. However, 12 of 18 FSA

security policies and procedures that we examined did not include evidence that they had been reviewed and updated at least annually, such as annotation of the updates in the documents' revision history. These included policies and procedures related to implementing access controls, security awareness and training, audit and accountability controls, security assessment and authorization, identification and authentication, and incident response, among others.

In addition, the agency did not always provide evidence that policies and procedures had been approved by security officials and disseminated to appropriate staff. Ensuring that security-related policies and procedures are reviewed and approved at least annually would help ensure that they continue to meet business needs and reflect the current practice of the agency. This in turn would ensure that the instructions with which agency officials are managing and executing the information security program are in line with the current information security environment and agency mission and operational requirements.

Further, 23 department-level Education security policies and procedures that we examined did not appear to have been consistently reviewed and updated in accordance with the department's defined frequency. These department-wide policies and procedures are applicable to FSA for its protection of its systems and information.

Consistent with this, in its November 2016 report on the department's implementation of FISMA, Education's Office of Inspector General identified weaknesses in the department's process for reviewing and approving policies and procedures.[47] Specifically, the Office of Inspector General noted that the policy and planning team was understaffed; the department had not effectively defined various document forms, such as guidance, handbooks, directives, and standard operating procedures; and the policy dissemination process needed to be improved. In addition, the Office of Inspector General reported that 27 information security-related policy documents were incomplete.

Accordingly, the Office of Inspector General made several recommendations to strengthen the department's policy and approval

[47]U.S. Department of Education, Office of Inspector General, *The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2016*, ED-OIG/A11Q0001 (Washington, D.C.: November 2016).

process. In July 2017, FSA officials told us that the Office of the Chief Information Officer had put corrective actions in place to address the outdated policies. However, until these actions are effectively implemented, department-level polices may continue to lack timely reviews and approvals. Further, the department, including FSA, risks having outdated polices that may not apply current security standards to its systems, including those that support the federal financial assistance program process.

In addition to outdated policies and procedures, the Education Inspector General continues to identify challenges in the department's implementation of its information security program. In its fiscal year 2016 report on metrics for FISMA implementation, the Inspector General noted that the department had established effective cybersecurity functions in two out of five functional areas established by federal guidance.[48] Moreover, the independent auditor's report for fiscal year 2016 identified persistent IT security control weaknesses as a significant deficiency for the department.[49] Further, in the 2017 report on the department's management challenges, the Inspector General continued to identify information technology security as one of its five challenges, and noted that security audits have continued to identify security controls that need improvement to adequately protect the department's systems and data.[50]

Most Schools Reported They Have Policies and Procedures for Managing and Protecting Federal Student Aid Information, but Selected

[48]These functional areas are identify, protect, detect, respond, and recover. See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, Md.: Feb. 12, 2014).

[49]U.S. Department of Education, *FY 2016 Agency Financial Report* (Nov. 14, 2016). A significant deficiency is a control deficiency, or combination of control deficiencies, in internal control that is less severe than a material weakness, but important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[50]U.S. Department of Education, Office of Inspector General, *FY 2017 Management Challenges* (October 2016).

Schools' Policies Did Not Address Federal Protection Requirements

Based on the results of our survey, we estimate that about 95 percent of schools have policies and procedures for managing federal student aid information, including guidance on record retention, disposition, and storage.[51] In addition, many of the schools reported having policies and procedures for protecting information, including the establishment of an information security program to secure student information. However, our review of selected school policies and procedures revealed that the policies did not always address the federal requirements for protecting student aid information.

Managing Student Information: Nearly All Schools Have Developed Record Retention Policies and Procedures

Based on the results of our survey, we estimate that 93 percent of schools have a policy regarding the retention of paper and electronic student aid records, and that 91 percent of them have a documented procedure for implementing the policy requirements. Further, based on the survey responses, schools that did not have their own records retention policies and procedures stated that they follow the retention policies developed by other entities, including those documented in Education's *FSA Handbook* and in the American Association of Collegiate

[51]We developed and administered a web-based survey to a generalizable stratified random sample of 560 schools from a population of about 6,200 schools. We took steps to ensure that our survey questions were clear and logical and that a financial aid administrator or other responsible official identified by FSA could answer the questions accurately and without undue burden. From the 560 selected institutions, we identified 21 out-of-scope schools (i.e., schools that were either closed or ineligible to provide federal student aid) and received valid responses from 349 of the 539 remaining in-scope schools. This represents an unweighted response rate of about 65 percent. All percentage estimates from our sample have margins of error at the 95 percent confidence level of plus or minus 12 percentage points or less, unless otherwise noted. Although we did not independently verify all survey responses, we determined the results to be sufficiently reliable to generalize to the full population of schools, See appendix I for more details.

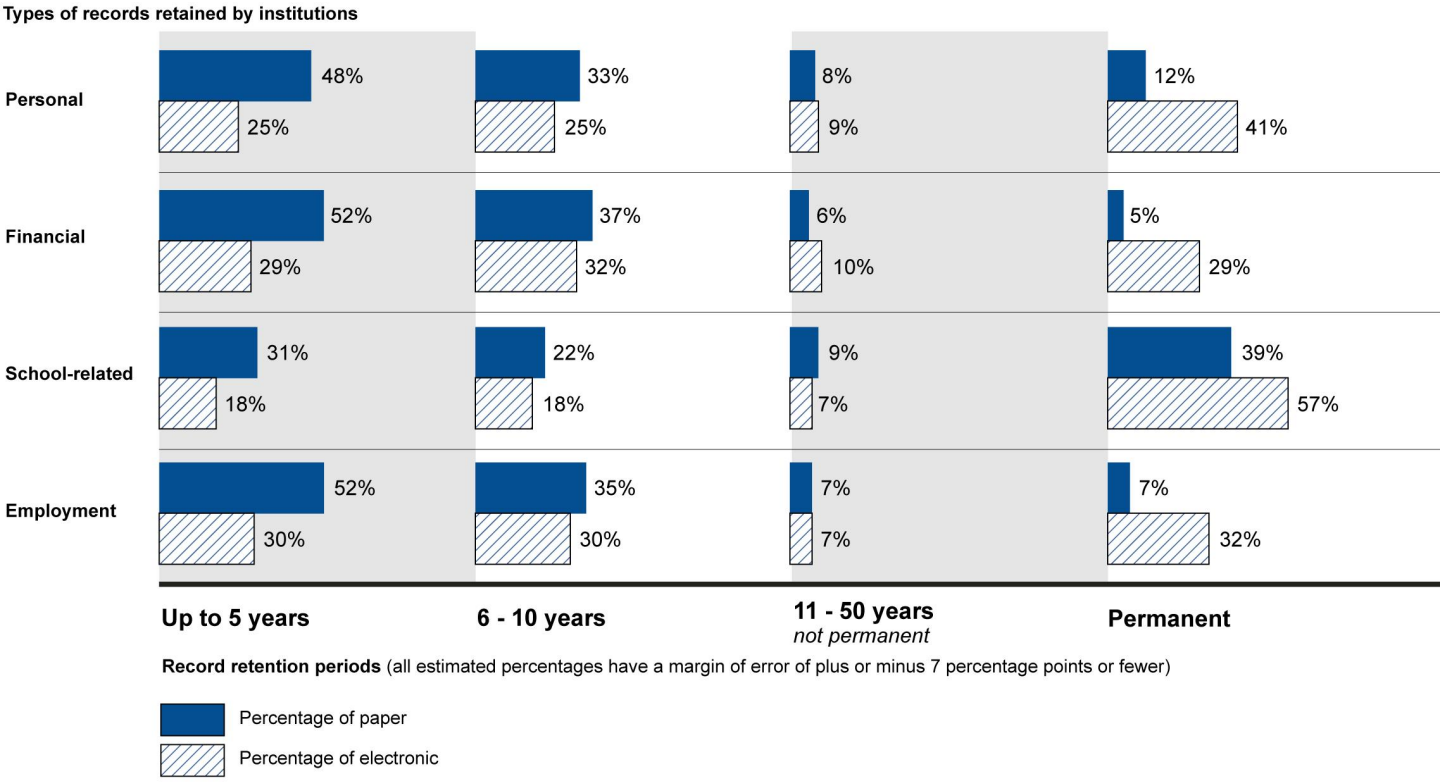
Registrars and Admissions Officers *Student Records Management: Retention, Disposal, and Archive of Student Records Guide*.[52]

In addition, the survey results revealed that schools vary in the retention of their paper-based and electronic student aid personal, financial, school-related, and employment information. Many schools retain paper-based personal (e.g., Social Security number, date of birth, citizenship), financial, and employment information for up to 5 years, and retain paper-based school-related information (e.g., degree, certificate, grade level, credit/clock hours) permanently.

For electronically stored information, the survey revealed that most schools retain financial information for 6 to 10 years, while personal, school-related, and employment information is retained permanently. The estimated retention periods by schools for the various types of paper-based and electronic records are illustrated in figure 6.

[52]The *FSA Handbook* is a publication intended for financial aid administrators and counselors who help students begin the aid process, verifying information, and making corrections and other changes to the information reported on the Free Application for Federal Student Aid. The American Association of Collegiate Registrars and Admissions Officers *Student Records Management: Retention, Disposal, and Archive of Student Records Guide* provides best practice recommendations to develop and modify student records management policy and practice for higher education officials.

Figure 6: Population Estimates for Schools' Retention Periods of Paper and Electronic Records by Information Types



Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

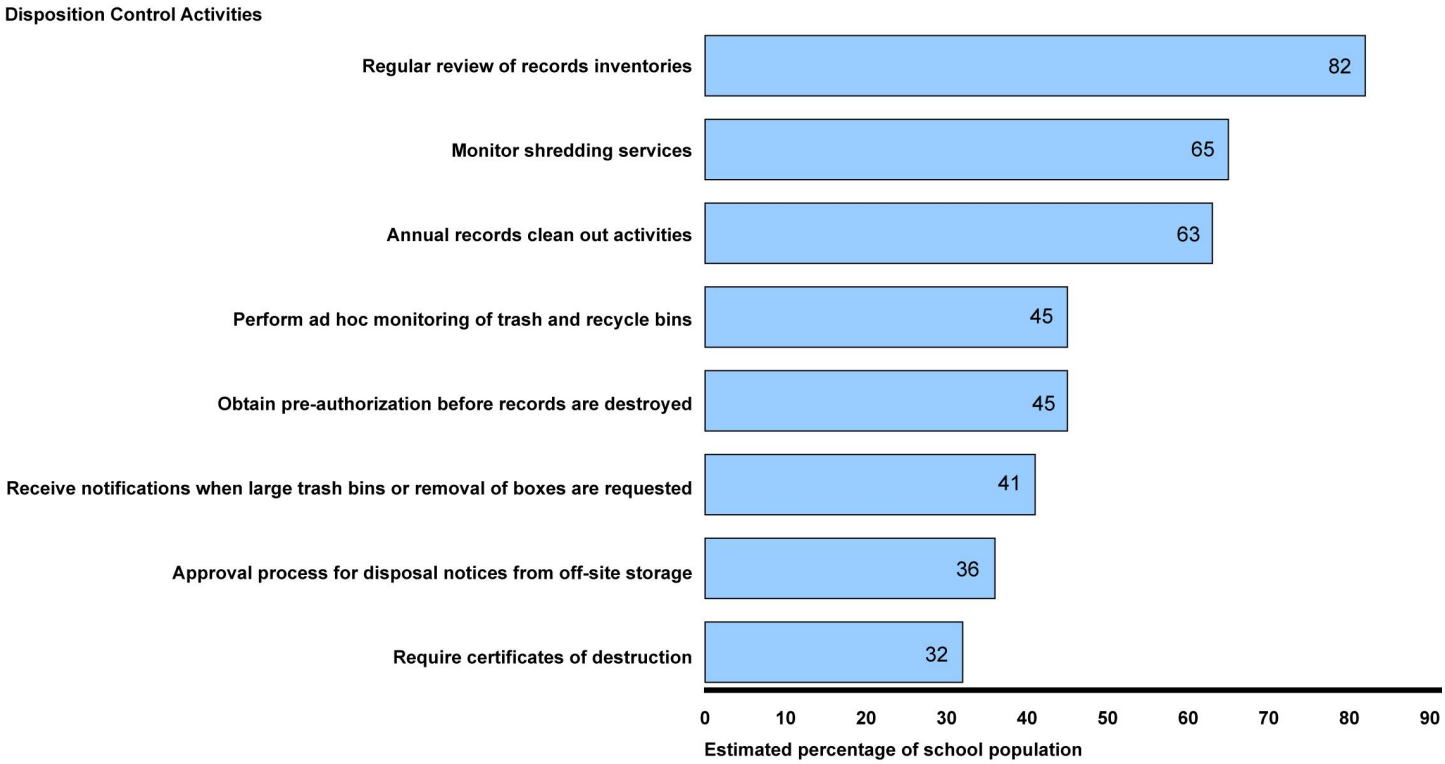
Note: Percentages do not add to 100 percent due to rounding.

Managing Student Information: An Estimated Three-Quarters of Schools Developed and Implemented Disposition Policies

We estimate that 77 percent of schools have developed policies that relate to the disposal of student aid information and that 70 percent have implemented the policies. Based on responses to our survey, schools that have not implemented these policies stated, among other things, that not enough time has elapsed to dispose of the student aid records, that records are kept permanently, or that the staff size was too small to handle the workload required to dispose of the records in a timely manner, which caused a backlog for several years.

Further, we estimate that 82 percent of schools are performing the regular review of records inventories control activity, identified by NARA for the destruction of paper-based and electronic student aid information. This activity involves schools transferring records of permanent, historical value for archival (preservation) and destroying all other records that are no longer needed for school administrative operations. In addition, we estimate that 65 percent of schools are monitoring shredding services, 63 percent are performing annual records clean-out activities, and 32 percent have certificates for the destruction of records. These control activities are important to ensure that federal student aid information is not destroyed prematurely or in error. Figure 7 shows the estimated use by schools of the NARA records' control activities.

Figure 7: Population Estimates of National Archives and Records Administration's Required Records' Disposition Control Activities Used by Schools



Source: GAO analysis of schools' survey data. | GAO-18-121

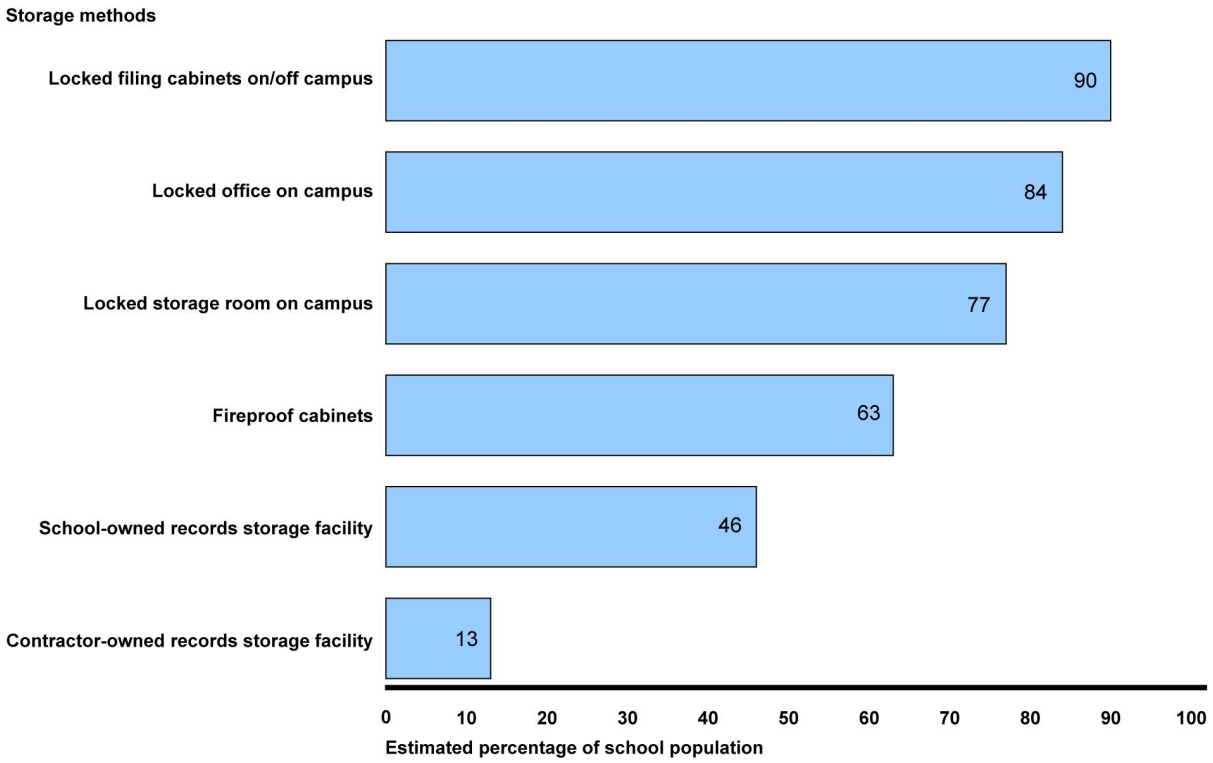
Note: Estimated percentages in this table have a margin of error of plus or minus 7 percentage points or fewer.

Managing Student Information: Almost All Schools Have Mechanisms for Storing Student Information

Among those schools participating in the federal student aid program, we estimate that 95 percent of them store student aid information electronically. Specifically, an estimated 92 percent do so using a data server on a school-owned network and an estimated 29 percent do so using a data server on a contractor-owned network.

In addition, we estimate that about 90 percent of these schools store paper-based student aid information. We also estimate that of the schools that store paper-based information, 77 percent do so using a locked storage room on campus, while 84 percent use a locked office on campus, 90 percent use locked filing cabinets, and 63 percent use fire-proof cabinets. Further, 46 percent store the information in school-owned records storage facilities and approximately 13 percent store the information in contractor-owned storage facilities (see figure 8).

Figure 8: Population Estimates of Federal Student Aid Record Storage Methods Used By Schools



Source: GAO analysis of schools' survey data. | GAO-18-121

Note: Estimated percentages in this table have a margin of error of plus or minus 7 percentage points or fewer.

Protecting Student Information: Selected Schools' Policies and Procedures Did Not Always Address Federal Requirements

Federal law establishes requirements for how schools are to protect student information with regards to information security. Under the Federal Trade Commission standards, financial institutions, such as schools, are to establish an information security program to secure customer information. Specifically, schools are to:

- Designate employee(s) to coordinate the information security program;
- Identify internal and external risks to the security, confidentiality, and integrity of student information;

- Design and implement safeguards to control risks identified in risk assessments;
- Evaluate and adjust the information security program based on results identified when testing or monitoring the effectiveness of safeguards' main controls, systems, and procedures; and
- Require service providers to implement adequate safeguards for customer information.

Our survey determined that most schools have policies and procedures for protecting federal student aid information. Specifically, in relation to the protection of student aid information, we estimate that 93 percent of schools have a documented information security program that includes policies and procedures for this purpose.

However, the policies and procedures that we reviewed of 123 schools randomly selected to provide documentation, did not always address federal requirements.[53] In reviewing documentation from these selected schools, we identified selected school policies and procedures that did not address the Federal Trade Commission requirements issued under the *Gramm-Leach-Bliley Act*, as required to participate in federal financial assistance programs. Specifically, 29 schools submitted documentation related to their information security programs, and our analysis of the documentation revealed that not all schools were adhering to the Federal Trade Commission requirements, as reflected in table 6.

[53]Unlike the responses to our survey, the results of our analysis of school-provided documentation are not generalizable to the population of schools.

Table 6: School Information Security Policies and Procedures That Met Federal Trade Commission Requirements

Requirement	Number of schools that met requirement
Designate employee(s) to coordinate the information security program	11 of 29
Identify internal and external risks to the security, confidentiality, and integrity of student information	11 of 29
Design and implement safeguards to control risks identified in risk assessments	12 of 29
Evaluate and adjust the information security program based on results identified when testing or monitoring the effectiveness of safeguards' key controls, systems, and procedures	10 of 29
Require service providers to implement adequate safeguards for customer information	8 of 29

Source: GAO analysis of selected schools' policies and procedures. | GAO-18-121

Specific elements that were not always fully addressed included the following:

- **Designation of program coordinator:** While 11 schools' policies addressed this element, the remaining 18 schools' policies did not. Of the 11 schools that adhered to the requirement, their policies designated various individuals including a chief information security officer and security architect, to coordinate the information security programs. The other 18 schools' policies did not designate coordinators of their information security programs.
- **Identification of risks to student information:** While 11 school policies included this requirement, the remaining 18 did not. Specifically, for those schools that included the requirement of external and internal risks to be identified as it relates to the security, confidentiality, and integrity of student information, their policies discussed assessing student information and the detection and response monitoring of student accounts. The remaining 18 schools' policies did not include the identification of risks to student information.
- **Design and implementation of security safeguards:** Twelve schools' information security policies addressed security safeguards to control risks, while 17 did not. For example, of those schools with policies that addressed the requirement, their security policies included the use of safeguards, such as password authentication, firewalls, and domain security to control among other things, user access levels to the network. However, for those schools that did not adhere to the requirement of the act, the policies did not include the design and implementation of security safeguards to control risks.
- **Evaluation and adjustment of information security program:** Ten schools' policies included the evaluation and adjustment of their

information security program based on results from safeguard testing or monitoring. These policies included the testing of the schools' information security programs and the results being reported to an executive director for any follow-up action and for recommendations to be implemented. The remaining 19 schools' policies did not include requirements to evaluate and adjust the information security programs based on safeguard testing and monitoring.

- **Requirement that service providers implement adequate safeguards by contract:** Of the 29 schools' information security policies, 8 addressed contractor implementation of safeguards, while 21 did not. Of those schools that included contractor implementation of safeguards, their policies included the school's role in overseeing and managing contracts with service providers and contractors demonstrating the ability to maintain appropriate safeguards for customer information. The other 21 schools' policy documentation did not include the requirement for service providers to implement adequate safeguards by contract.

Although the results of our review of selected school policies and procedures are not generalizable to the full population of schools that participate in the federal financial assistance program, it does raise concerns about the protection of federal student aid information. It will be important for FSA to ensure that schools are protecting federal student aid information in accordance with the *Gramm-Leach-Bliley Act* (which we discuss in the next section).

Methods Used by FSA to Provide Oversight of Schools Do Not Include Assessing the Protection of Student Information

The *Higher Education Act* gives Education responsibility for overseeing schools to ensure that they are eligible and can continue to participate in federal financial assistance programs. Education does this, in part, by requiring the schools to demonstrate their administrative capability. To do so, a school must, for example, administer its federal financial assistance program in accordance with all statutory provisions of the *Higher*

Education Act, and meet the requirements included in Education's regulation for demonstrating administrative capability.[54]

Once a school is able to demonstrate that it meets the requirements for administrative capability, it then enters into program participation agreements with the department as a prerequisite to receiving federal student aid funding. The agreements include terms and conditions, in which schools are required to understand, agree to, and comply with applicable statutes and regulations, including establishing information security programs in accordance with the Federal Trade Commission Standards for Safeguarding Customer Information under the *Gramm-Leach-Bliley Act*.

The *Higher Education Act* also instructs the Secretary of Education to conduct program reviews of participating schools. While Education cannot conduct program reviews of every school, it must prioritize the reviews to focus on schools that meet certain criteria, such as those that pose a significant risk of failure to comply with the act's requirements for administrative capability or financial responsibility, as determined by the Secretary, among other factors.[55]

Further, GAO's *Standards for Internal Control in the Federal Government* call for an entity's management to conduct activities to monitor and evaluate program performance.[56] The monitoring of a program's performance is essential to help keep initiatives aligned with changing objectives, environment, laws, resources, and risks.

[54]To demonstrate its administrative capability a school must, for example, have a number of adequate qualified persons to administer the financial aid assistance program in which the school participates, and have written procedures or information indicating the responsibilities of various offices with respect to the approval, disbursement, and delivery of federal financial assistance, among other requirements.

[55]Other factors for determining the priority of program reviews include, for example, (1) have a loan cohort-default rate in excess of 25 percent or have a loan-default rate that places the school in the highest 25 percent of defaulting institutions; (2) have a loan-default rate in dollar volume that places the school in the highest 25 percent of defaulting institutions; and (3) have deficiencies or financial aid problems reported by the State licensing or authorizing agency, or by the appropriate accrediting agency or association.

[56]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sep 10, 2014).

FSA performs oversight of schools compliance with certain statutory and regulatory requirements identified within the participation agreements. To carry out Education's oversight responsibilities, FSA's Program Compliance Office conducts program reviews to confirm that schools meet agreed-upon terms and conditions outlined in program participation agreements. The terms and conditions address federal requirements outlined in the *Higher Education Act*, and the *Code of Federal Regulations* for institutional eligibility, financial responsibility, and administrative capability, among other requirements.

Each year, FSA selects a number of schools to receive these program reviews. This selection is based on several criteria and risk factors specified in FSA's program review instructions. These selection criteria include, among others, significant fluctuations in federal financial assistance funding, loan default rates, accreditor adverse actions, dropout rates, and frequent changes in school officials. In selecting schools for review, FSA also relies on the findings of schools' required annual financial statements and compliance audits.[57]

During the program review, FSA's reviewers perform financial analyses and monitor financial status; schedule and conduct compliance initiative reviews, as needed; and monitor schools and their agents through on-site and off-site reviews and analysis of various reports to provide early warning of program compliance problems. The reviews also identify actions schools must take to improve their future administrative capabilities.

After completing a program review, FSA issues a Final Program Review Determination report to schools, which includes review findings, the school's responses to the findings, and the Education's final determination. The Final Program Review Determination report also

[57] The compliance audits, as required by the *Higher Education Act* (as amended), dictate that schools are to submit to the Secretary of Education a financial and compliance audit report that is conducted by a qualified, independent organization or person. When performing these audits, nonprofit and public schools are to follow guidance contained in the OMB *2 CFR Part 200, Appendix XI, Compliance Supplement*, and for-profit schools are to follow audit guides developed by and available from Education's inspector general. Both guides include audit objectives and procedures for evaluating compliance with requirements related to federal financial assistance programs. The documents outline areas to be assessed within the audits including, among other things, the school's eligibility and participation, disbursements, return of federal financial assistance program funds, and cash management.

identifies liabilities, if any, calculated based on the findings of the program review; provides instructions for the payment of liabilities, as appropriate; notifies the school of its right to appeal the existence and amount of any liabilities identified, as appropriate; and closes the program review, if appropriate.

However, FSA currently does not have an oversight mechanism for ensuring that schools adhere to the Federal Trade Commission protection requirements. Specifically, FSA's program review process does not consider schools' protection of student information despite schools agreeing to adhere to this requirement by signing a program participation agreement. As noted previously, schools are required to establish information security programs to protect student aid information in accordance with the Federal Trade Commission *Standards for Safeguarding Customer Information* under the *Gramm-Leach-Bliley Act*. FSA officials acknowledged that, while this requirement exists, the agency has not requested that schools report information related to their protection of student information.

According to FSA officials responsible for oversight activities, the security of student information has not been reviewed largely because the independent annual compliance audits guidelines of OMB and the Education Office of Inspector General, used by schools to demonstrate their administrative capabilities, do not include a requirement for reviewing schools' information security programs. Rather, the audits focus on areas to be assessed that include, among other things, the school's eligibility and participation, disbursements, return of federal financial assistance program funds, and cash management—none of which relate to the protection of student information.[58]

To address this shortfall, FSA officials stated that, in December 2016, the Program Compliance Office within FSA requested that OMB include the testing of schools' adherence to information security program requirements in a future revision of audit guidance contained in the OMB *Compliance Supplement*. In April 2017, FSA similarly requested that Education's Office of Inspector General include this requirement in its

[58]The12 areas to be selected for assessments are: (1) activities allowed or unallowed, (2) allowable costs/cost principles, (3) cash management, (4) eligibility, (5) equipment and real property management, (6) matching, level of effort, earmarking, (7) period of performance, (8) procurement and suspension and debarment, (9) program income, (10) reporting, (11) subrecipient monitoring, and (12) special tests and provisions.

audit guidance covering for-profit schools. In both instances, FSA requested that guidance provide information on audit objectives and suggested procedures to follow, which include to

- verify that a school has designated an individual to coordinate the information security program,
- obtain the school's risk assessment and verify that it addresses the required standards for safeguarding customer information, and
- obtain documentation of the school's safeguard that aligns with each risk identified from the risk assessment and verify that the school has identified a safeguard for each risk.

According to Education's Assistant Inspector General for Audit, the Office of Inspector General, along with the Office of the Chief Financial Officer and the Office of the Chief Information Officer, are working with OMB to develop audit steps that would include evaluating schools' adherence to the Federal Trade Commission information security program requirements.[59] According to an FSA official, the anticipated update to the OMB *Compliance Supplement* is planned for 2019. Once the supplement is updated, according to the Assistant Inspector General, the Office of Inspector General intends to modify its guide. However, in the absence of OMB's revised audit guidelines or its own oversight mechanism to evaluate schools' adherence to the Federal Trade Commission's requirements, FSA lacks assurance that schools have effective information security programs in place. Ensuring that information security considerations are included in its program review process would provide FSA with a means of gaining greater insight into whether schools are adequately protecting student PII shared with them as part of the student federal financial aid process, even in the absence of OMB's guidelines. Moreover, doing so would be consistent with GAO's *Standards for Internal Control in the Federal Government*, which calls for an entity's management to conduct activities to monitor and evaluate program performance to help keep initiatives aligned with changing objectives, environment, laws, resources, and risks.

[59]The Assistant Inspector General also added that the information security requirements were intended to be added to the updated audit guides in 2017. However, schools that have not yet signed revised program participation agreements raised concerns about the additional costs that would be incurred when contracting with audit firms that have expertise in information security as well as financial audits.

Another factor that may contribute to the lack of attention to information security in FSA's oversight process is that statutes and implementing regulations do not focus on these requirements. Specifically, schools are not required by statute or implementing regulation to demonstrate their adherence to the Federal Trade Commission *Standards for Safeguarding Customer Information*, under the *Gramm-Leach-Bliley Act*, as part of demonstrating their administrative capability. This is despite the Secretary of Education's consideration of any breach to the security of student records and information as a demonstration of a potential lack of administrative capability.[60]

At the same time Education is not performing this oversight, schools are reporting information security breaches. For example, 13 schools reported physical and electronic data breaches to Education from November 2013 to December 2016. These breaches included students' PII data being available for public viewing; a stolen laptop that contained students' names, address, and transcript information; loan notices being sent to students other than the borrower with personal information such as names, addresses, Social Security numbers, and loan amounts; and student medical files removed during a school building break-in.

The recent reported data breaches, weaknesses noted in selected schools' security policies, as well as increasing cyber threats, raise concerns about FSA's oversight and how effectively schools are protecting student aid information. Requiring schools to demonstrate, as part of their administrative capability, the ability to protect federal student aid data, could keep the public, and Education better informed of schools' efforts in this area.

Conclusions

The federal student aid process is complex and involves the collection of large amounts of personal information from millions of American families each year. FSA relies extensively on IT systems to collect, process, and share this information. It is, therefore, important that FSA have processes in place for effectively managing and protecting the information it collects, uses, and shares.

[60] 34 C.F.R. 668.16(c)

While Education's and FSA's policies for records management and protection of sensitive information generally align with federal requirements, weaknesses in some processes limit their effectiveness. Specifically, FSA had not fully established procedures for meeting records management requirements, including establishing disposition schedules for key systems; establishing procedures for efficiently disposing of electronic records; documenting procedures for incorporating records management requirements into electronic information systems; ensuring regular records management training for staff; and conducting regular, in-depth triennial assessments. In addition, FSA has not ensured that PIAs contain sufficient and consistent details or that its information security policies are up to date. Until FSA updates its policies and procedures and ensures that PIAs are sufficiently detailed, student aid records may be at unnecessary risk. Further, the agency will lack assurance that privacy risks have been sufficiently considered and addressed when it collects, uses, and shares PII.

Although schools generally had policies and procedures for managing student aid information, selected school policies did not always meet the federal requirements for establishing an information security program, as required by schools signing program participation agreements. These concerns are heightened by FSA's limited oversight in ensuring that schools implement requirements for the protection of students' data. Strengthening the oversight process by incorporating information security requirements would provide greater assurance that the personal student information shared with schools is being effectively protected.

Recommendations for Executive Action

We are making seven recommendations to the Department of Education to take steps to ensure the effective management and protection of student aid records. Specifically:

The Secretary of Education should direct the Chief Operating Officer of FSA to establish and document a procedure for the destruction of records contained in electronic systems in accordance with approved disposition schedules.
(Recommendation 1)
The Secretary of Education should direct the Chief Operating Officer of FSA to ensure staff receive records management training annually.
(Recommendation 2)

The Secretary of Education should direct the Chief Operating Officer of FSA to conduct the triennial assessment of the FSA records management program.
(Recommendation 3)

The Secretary of Education should direct the Chief Operating Officer of FSA to ensure that privacy impact assessments address all required elements.
(Recommendation 4)

The Secretary of Education should direct the Chief Operating Officer of FSA to ensure that information security-related policies and procedures are reviewed at least annually, in accordance with FSA policy; updated as needed; and approved by security officials.
(Recommendation 5)

The Secretary of Education should incorporate into its program review process the review of postsecondary schools' information security program requirements.
(Recommendation 6)

The Secretary of Education should update its regulation to include protections of personal information as an element of a school's ability to demonstrate its administrative capability.
(Recommendation 7)

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Department of Education. In its comments (reprinted in appendix III), the department concurred or generally concurred with five of our recommendations, partially concurred with one recommendation, and did not concur with another.

Among the four recommendations with which it concurred, the department described various actions that it had taken or planned to implement them. Specifically, the department stated that it had made the following efforts:

- Completed its fiscal year 2017 mandatory records management training on September 30, 2017 and will continue to require annual records management training of its FSA staff.

- Completed the data collection phase of the 2017 organization-wide internal records management self-assessment on September 30, 2017, and expects to complete the process by December 31, 2017.
- Developed a new template for PIAs that reflects current OMB requirements. The department also said it published a policy in 2016 which states that PIAs must be reviewed whenever a system change creates a new privacy risk and at least every 2 years, among other requirements. Further, it stated that, since the policy update, the department's Office of the Chief Privacy Officer has asked all Principal Offices to review their systems and associated PIAs and determine if updates are needed. If updates are needed, the office asks the Principal Office to update its PIAs with the new template that includes all the required elements. If an update is not required, the owner of the system can certify that the PIA is valid as written.
- Ensured that information security-related policies and procedures are reviewed at least annually, in accordance with FSA policy; updated as needed; and approved by security officials. The department added that it and FSA have efforts under way to review and update these policies and procedures and intend to work together to conduct an annual review of their respective information security policies.

We intend to follow up with the department and FSA to obtain and assess the evidence supporting their implementation of these recommendations.

With regard to our recommendation that the department incorporate into its program review process the review of postsecondary schools' information security program requirements, the department generally agreed that information security needs to be better reflected in its oversight of schools. However, given the upcoming updates to OMB's and the Education Office of Inspector General's audit guidance, the department stated that it believes the annual compliance audit process is more appropriate, and will promote better consistency and implementation over time, than the program review process. The department added that, in the interim, FSA staff will take follow-up actions when the information security program issues for a postsecondary school are identified during an FSA program review, either through program review staff observations or discussions with school staff. Further, it stated that FSA will update its program review process manual to reflect these procedures and will also consider including information security issues as part of program reviews or other monitoring and oversight through the use of surveys or sampling.

We agree that using the results of audits conducted with the expected guidance to inform program reviews should enhance FSA's oversight of schools' information security programs. In addition, taking the interim steps described could provide FSA with additional insight into information security issues at schools. If the expected guidance is implemented effectively, we believe these actions would meet the intent of our recommendation.

The department partially agreed with our recommendation to establish and document a procedure for the destruction of records contained in electronic systems, in accordance with approved disposition schedules, because it believes FSA already has appropriate procedures in place. Specifically, the department stated that our draft report had comingled the process for the destruction of structured records (e.g., data files in its electronic information systems) and unstructured records (e.g., electronic agency policy documents), which resulted in our inaccurate assessment of one process instead of two distinct processes. While we acknowledge that the department has two distinct processes for its two types of electronic records, our review focused on the electronic systems and structured data that are used to the support the federal financial aid assistance process, as discussed in the report.

Regarding its records contained in data files in its electronic information systems (that is, the structured data), the department stated that those records are managed through its Lifecycle Management Methodology process that covers structured data systems from initiation throughout system life, including change management, and closing with systems' retirement. The department added that, as a result of our audit, it would, nevertheless, conduct a review of FSA systems to assess if structured data are being retained beyond the scheduled destruction date calculation.

As we discuss in our report, however, the documentation of FSA's Lifecycle Management Methodology does not specifically or clearly address the disposition of records contained in electronic data files, in accordance with established retention periods. Rather, the guidance addresses the retirement of systems, as noted by the department, and it does not describe the steps for approving and carrying out the deletion of data files that have reached the end of their retention period, whether or not this coincides with the retirement of a system. Similar to the process that FSA has established for physical records, developing a procedure for the destruction of student aid records in electronic information systems would provide assurance that these sensitive records are not being

retained beyond their scheduled destruction date and the increased risk for the potential of unintended disclosure. Thus, we believe our recommendation is still warranted.

The department did not concur with our recommendation to update its regulation to include protections of personal information as an element of a school's ability to demonstrate its administrative capability. According to the department, the Higher Education Act of 1965, along with the requirements to comply with the Federal Trade Commission's Standards for Safeguarding Information, contained in schools' program participation agreements, provide the department with sufficient authority to require schools to protect personal information as an element of their ability to demonstrate administrative capability.

While we agree that there are requirements for schools to protect student aid information and that FSA has authority to require schools to protect information, neither the Federal Trade Commission regulation nor FSA require schools to demonstrate their adherence to information security requirements when they initially apply to participate in federal student financial aid programs, or as a condition for receiving continuing approval from FSA to participate in the financial assistance programs. Moreover, schools are to demonstrate, among other things, administrative capability. By including the protections of personal information as a requirement for schools in demonstrating their administrative capability, FSA would have better insight and the schools would be better able to protect student information, including PII. Thus, we maintain that our recommendation is appropriate.

Beyond the aforementioned comments, Education also provided technical comments on the report, which we have incorporated, as appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees, the Secretary of Education and other interested parties. In addition, this report is available at no charge on the GAO website at http://www.gao.gov.

Should you or your staffs have any questions on information discussed in this report, please contact Nick Marinos 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 major contributions to this report are listed in appendix IV.

Nick Marinos
Director, Cybersecurity and Information Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to: (1) describe how the Office of Federal Student Aid (FSA) and schools use the information they collect in managing the student financial assistance program; (2) determine the extent to which FSA policies and procedures for managing and protecting federal student aid information align with federal requirements and guidance; (3) describe the extent to which schools have established policies and procedures for managing federal student aid information; and (4) determine the extent to which FSA ensures that schools protect federal student aid information in accordance with federal requirements and guidance.

To address the first objective, we obtained and reviewed documentation that described the federal student aid program and the types of information being collected, used, and shared in the process. Specifically, we reviewed the Free Application for Federal Student Aid form to identify the types of information, including personally identifiable information (PII), being collected from students and parents. We also obtained and reviewed the federal student aid handbook of financial aid administrators to better understand the federal student aid process. Further, we reviewed Department of Education (Education) and FSA information collection requests forms, system of records notices, privacy impact assessments (PIA), and descriptions of automated systems used to manage the student aid process in order to identify and describe how the information being collected was used throughout the federal student aid process. We also interviewed FSA system owners to better our understanding of how federal student aid information, including PII, is collected, used, and processed.

To address our second objective, we reviewed Education and FSA policies and procedures to determine the extent to which they meet federal requirements, as well as other standards and guidance, to provide for the management and protection of federal student aid data. Specifically, we reviewed policies and procedures related to records management, including for the storage and disposition of records; protecting PII; and securing agency information systems.

Regarding records management, we reviewed Education and FSA policies and procedures to determine the extent to which they meet requirements established in the *Federal Records Act*, National Archives

and Records Administration (NARA) implementing regulations, and other NARA guidance. The policies and procedures reviewed included Education's directive on records management, directive on records retention and disposition schedules, records liaison officers' *File Plan Manual*, steps for transferring records, and records disposal notification report processes.

Further, we identified requirements assigned to FSA by Education policies for implementing key records management responsibilities and reviewed documents and artifacts to determine if FSA had processes in place for carrying out these responsibilities. To make this assessment, we reviewed FSA documentation, including records disposition schedules, office file plan, procedures for transferring and disposing of records, training slides and documentation of employees' completion of training, and documentation of the results of FSA's records management self-assessment. We also identified disposition and retention periods for records containing student information and PII information. For each requirement, we determined if FSA provided evidence through documentation and artifacts it had developed that it had addressed all aspects of the requirement, part of the requirement, or none of the requirement.

Regarding the protection of PII collected and used during the federal student aid process, we focused on key privacy requirements established by the *Privacy Act of 1974* and the *E-Government Act of 2002*, along with Office of Management and Budget (OMB) guidance on agency privacy responsibilities, and the *Uniform Administrative Requirements*, *Cost Principles*, and *Audit Requirements for Federal Awards, 2 CFR Part 200, Appendix XI, Compliance Supplement*. The policies reviewed included Education's directives on the *Privacy Act of 1974* and the *E-Government Act of 2002*, its information assurance and cybersecurity handbook, and its breach notification and response policy and plan. Specifically, we reviewed Education policies and procedures to determine if they addressed the requirements imposed on agencies by the *Privacy Act*, *E-Government Act*, and OMB, such as designating a senior agency official for privacy and developing system of records notices and PIAs.

We reviewed FSA documentation to determine if it had processes in place for carrying out responsibilities relating to privacy as established by Education policy and other requirements. Specifically, we reviewed FSA's system of records notices and determined if they contained elements required by the *Privacy Act*; PIAs for FSA's systems to determine if they included elements called for by OMB guidance; training materials and

documentation of employees' completion of training; and other policies and procedures related to the identification and protection of PII. In addition, we determined if FSA had published a privacy policy on its website, along with *Privacy Act* notices for web-based applications that collect PII. For each requirement, we determined if FSA provided evidence that it had addressed all aspects of the requirement, part of the requirement, or none of the requirement.

To determine how FSA is securing agency information systems, we reviewed Education Office of Inspector General reports on the department's information security program and major management challenges more generally. We identified and summarized challenges, findings, and recommendations identified by the Office of Inspector General that pertain to information security weaknesses at the department.

We also reviewed Education and FSA policies and procedures and compared them to guidance from the National Institute of Standards and Technology (NIST) for establishing policies, procedures, and processes to manage and monitor an organization's management of information security. Specifically, we determined if the department had established policies and procedures for selecting and implementing information security controls from the control families identified in NIST's *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4. For the selected control families, we determined whether Education and FSA had: (1) developed, documented, and disseminated (a) policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) procedures to facilitate the implementation of the policy and associated controls; and (2) reviewed and updated the policy and procedures at an organization-defined frequency. For each control area we determined if the department had provided evidence sufficient to fulfill criteria in its entirety; provided evidence that indicates that efforts have begun to fulfill the criteria, but not in its entirety; or provided no auditable documentation to fulfill the criteria. This assessment was limited to the establishment of policies and procedures; we did not assess the extent to which Education and FSA had implemented their information security program or specific security controls.

For each of these areas—records management, privacy, and information security—we supplemented our review and confirmed our findings through written questions to and responses from FSA and Education

officials with records management, privacy, and information security responsibilities, as well as in-person interviews.

To address our third objective, we administered a web-based survey from November 2016 to March 2017 to a generalizable stratified random sample of 560 schools from a population of about 6,200 schools. Our survey questionnaire asked schools fixed-choice questions about their policies and procedures in place to manage and protect student aid information collected. In addition, it asked for descriptive written responses to open-ended questions regarding how schools ensure effective retention, storage, and disposition of federal student aid information and how schools ensure that appropriate controls are in place to safeguard the federal student aid information it collects and uses.

To ensure that our questions were clear and logical and that respondents could answer the questions without undue burden, we pre-tested the draft survey with three schools that were part of our stratified random sample. We then made changes to the survey based on their experiences taking the test survey in advance of sending the survey to the selected schools.

We began survey fieldwork by e-mailing the web survey link and unique login information to the financial aid administrator or other responsible official identified by Education's Office of Federal Student Aid for each sampled school. Thirty-four of the schools were affiliates and connected to other schools in our survey, which we divided into six groups. Specifically, the schools in each group shared common information management policies and procedures, so questionnaires for schools in each of these groups were directed to one respondent, who in some cases provided a single response applicable to all of their schools. Throughout fieldwork, we made up to two follow-up contact attempts by e-mail and additional telephone contact attempts with those who had not yet made valid responses.

From the 560 selected schools we identified 21 "out of scope" schools (i.e., schools that were either closed or ineligible to provide federal student aid) and received valid responses from 349 of the 539 remaining in-scope schools. This represents an unweighted response rate of about 65 percent. The weighted response rate, which accounts for the differential sampling fractions within strata, is 61 percent. The disposition of the survey respondents is described in table 7.

Table 7: Description of Sample Frame, Stratification, and Response Rates for the Stratified Random Sample of Schools

Stratum	Population size	Sample size	Valid responses	"Out of scope" schools
1="Largest 40 schools (total enrollment)"	40	40	31	0
2="Public - 4 year"	657	48	28	0
3="Public - 2 year or less"	1,212	86	50	1
4="Private, Nonprofit- 4 year"	1,566	118	73	4
5="Private, Nonprofit - 2 year or less"	206	18	10	1
6="Private, For Profit - 4 year"	314	22	10	6
7="Private, For Profit - 2 year or less"	1,860	115	62	8
8="Foreign - 4 year"	402	112	84	1
9="Foreign - 2 year or less"	1	1	1	0
Total	**6,258**	**560**	**349**	**21**

Source: GAO analysis of Department of Education data. | GAO-18-121

We conducted an analysis of our survey results to identify potential sources of nonresponse bias by examining the response propensity of the sampled schools based several demographic characteristics. These characteristics included school types (Public, Private Nonprofit, Private For Profit, and Foreign), program lengths (4 years and 2 years or less) and regional location. Further, we conducted statistical tests of differences between weighted proportion estimates generated from the sample of respondents for these characteristics to the proportion of schools in the sampling frame.

The results of this nonresponse bias analysis showed no significant differences in response propensities or between known population proportions and estimates for nearly all of the characteristics we examined. We identified that schools in the northeast were slightly underrepresented in our sample of respondents but did not identify any systemic differences in survey estimates for several key survey questions. Based on these results and the 61 percent weighted response rate, we determined that weighted estimates generated from these survey results are generalizable to the population of eligible schools and are sufficiently reliable for the purposes of this report.

Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our particular sample's results as a 95 percent confidence interval (e.g., plus or minus 7 percentage points). This is the interval that would contain the actual

population value for 95 percent of the samples we could have drawn. As a result, we are 95 percent confident that each of the confidence intervals in this report will include the true values in the study population. All percentage estimates from our sample have margins of error at the 95 percent confidence level of plus or minus 12 percentage points or less, unless otherwise noted.

Further, we asked 123 schools randomly selected from the 560 schools in our sample to provide documentation of their policies and procedures for managing federal student aid information. Of these 123 schools, 44 submitted documentation. We assessed this documentation to determine whether the policies and procedures addressed how student aid information is accessed, used, and protected; how long student aid information is retained; how student aid information is disposed; and whether an information security program was developed in accordance with federal standards for safeguarding customer information. Unlike the responses to our survey, the results of our analysis of school-provided documentation are not generalizable to the population of schools.

The practical difficulties of conducting any survey may introduce errors, commonly referred to as non-sampling errors. For example, differences in how a particular questions is interpreted, in the sources of information available to respondents, or in how the data were processed and analyzed can introduce unwanted variability into the results. With this in mind, we took a number of steps to minimize these factors. For example, our survey was developed in collaboration with a GAO methodologist, survey specialists, and statisticians, and the questions were tested to minimize the likelihood of measurement error. Multiple contact attempts were made by e-mail and telephone to reduce the extent of nonresponse-related error. Data processing and analysis programming was independently verified to avoid processing error.

For our fourth objective, we reviewed applicable laws and regulations that describe the requirements and priority that the Secretary of Education is to give when conducting school program reviews. We also reviewed the *Gramm-Leach-Bliley Act,*[1] which describes requirements for the protection of nonpublic personal information and the Federal Trade Commission's *Standards for Safeguarding Customer Information*[2]

[1]Pub. L. No. 106-102, Title V, Subtitle A.

[2]16 C.F.R. Part 314.

regulation, which sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. We then compared the requirements of the statute and regulation to FSA's program review documentation, including its program review procedures and fiscal year 2017 program review instructions, which described their school program review and risk assessment process. We also reviewed OMB's *Compliance Supplement* and Education's Office of Inspector General guide for audits of proprietary schools to analyze and compare the assessment requirements to the requirement standards of safeguarding customer information, including records management, security, and privacy that independent auditors are to follow in conducting compliance audits at schools. We supplemented our document reviews and analysis with interviews with FSA's Financial Institution Oversight Service Group.

We conducted this performance audit from December 2015 to November 2017 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: Automated Systems Involved in the Federal Financial Assistance Programs Process

The federal financial assistance program process involves multiple participants and automated systems, and can be explained in four phases: (1) school eligibility determination, (2) student application and eligibility determination, (3) disbursement of funds, and (4) repayment and collection of loans. The automated systems listed in table 9 are involved in one or more of these phases, and collect and process various types of student aid information. The information is then used by FSA, schools, and other stakeholders, including federal agencies, to determine aid eligibility, types and amounts of aid that students are able to receive, and the distribution and repayment of loans.

Table 8 describes the systems used in FSA's financial assistance process.

Table 8: Description of Systems Used in the Office of Federal Student Aid (FSA) Financial Assistance Process

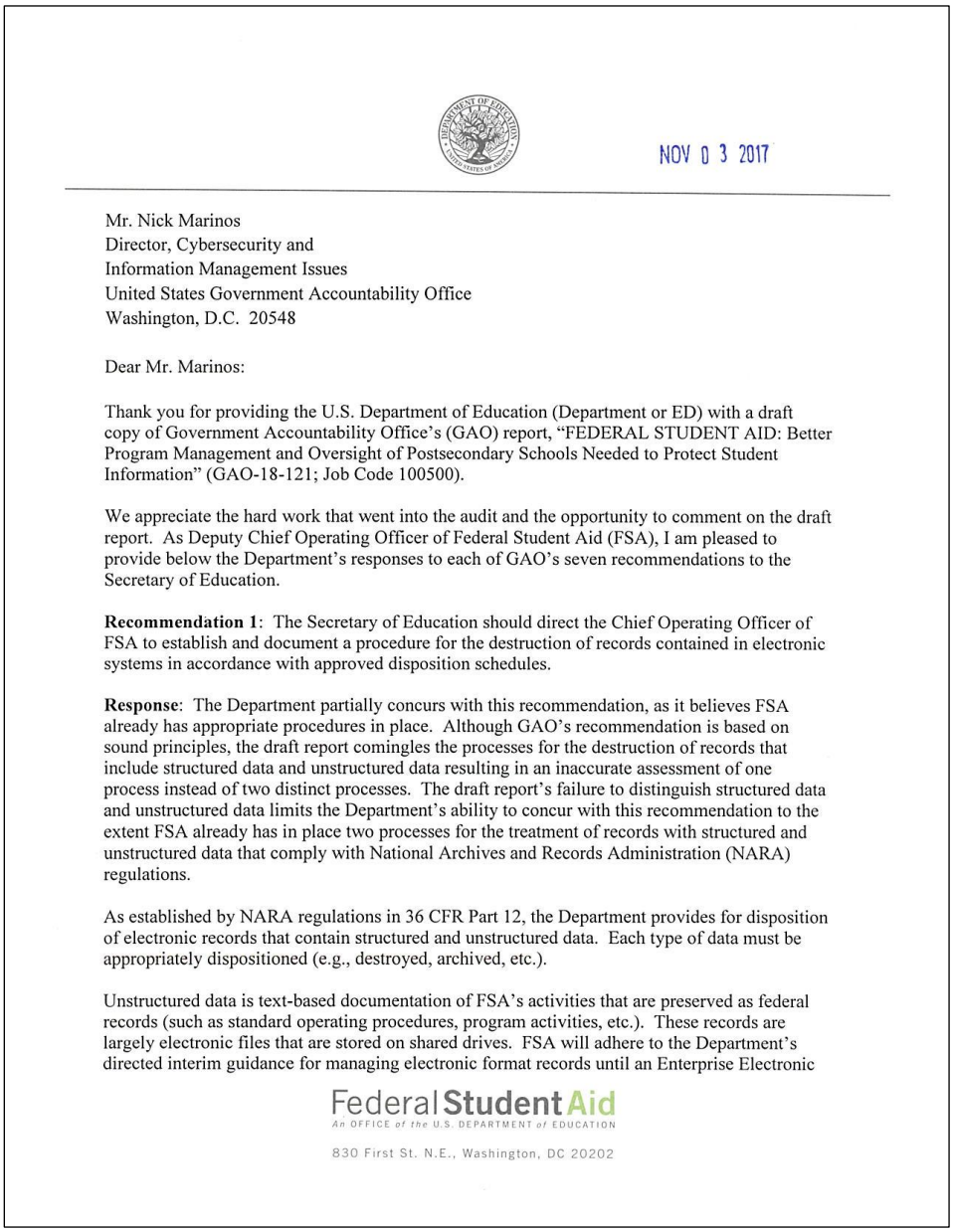
System	Description	Phase	Types of information collected
Central Processing System	Processes all applications for FSA, calculates financial aid eligibility and notifies students and educational institutions of the results of the eligibility calculation	1, 2, 3	Student demographics, student eligibility, student finances, parent demographics, parent finances
Common Origination and Disbursement system	Initiates and tracks the disbursement of funds to eligible students and schools for financial aid programs such as Pell Grant, Teacher Education Assistance for College and Higher Education Grant, and Direct Loan programs, among others.	1, 2, 3, 4	Student demographics, student finances, parent demographics, parent finances
eCampus-Based system	Allows schools to submit the Fiscal Operations Report and Applications to Participate in campus based programs, such as the Federal Perkins Loan Program, Federal Supplemental Educational Opportunity Grant Program and Federal Work-Study Program	1	
Electronic Application for Approval to Participate	Allows schools to apply for designation as an eligible institution to participate in the Federal Student Financial Aid Programs.	1	
EZ-Audit system	Provides schools with a paperless, single point of submission, for audited financial statements and compliance audits required by Title IV participants.	1	

System	Description	Phase	Types of information collected
Financial Management System	Works with the grant management system to communicate financial information and to deliver federal funding to schools. This is the general ledger for FSA.	3	Student demographics, student finances, parent demographics, parent finances
Grant Management system	Allows schools to request payment for the following programs: Federal Pell Grant, Iraq and Afghanistan Grant, TEACH Grant, Federal Supplemental Educational Opportunity Grant, Federal Work-Study, Federal Perkins Loan, and Direct Loan Program.	3	Financial information
National Student Loan Data System (NSLDS)	Provides schools, guaranty agencies, lenders and students with a centralized, integrated view of federal student aid loans and Pell grants and tracks them through their entire life cycle.	1, 2, 3, 4	Student demographics, student finances
Postsecondary Education Participants System	Maintains eligibility, certification, demographic, program review, financial, and audit review and default rate data about institutions, lenders and guarantors participating in the Title IV programs.	1, 2	Student demographics
Student Aid Internet Gateway	Allows FSA partners to securely exchange batch data with FSA application systems, such as the Common Origination and Disbursement system, the Central Processing System, and the National Student Loan Data System.	1, 2, 3	Student demographics
Student Aid Internet Gateway Participation Management	Allows organizations to enroll for electronic access to FSA systems.	1	Student demographics, parent demographics

Source: GAO analysis of Department of Education, Office of Federal Student Aid data. | GAO-18-121

Note: Phase 1 refers to the time period during which school eligibility determination occurs; Phase 2 refers to the time period during which student application and eligibility determination occur; Phase 3 refers to the time period during which disbursement of funds occurs; Phase 4 refers to the time period during which repayment and collection of funds occur. (For more details on the four phases, see earlier sections on each phase, and figure 1.)

Appendix III: Comments from the Office of Federal Student Aid, Department of Education



NOV 0 3 2017

Mr. Nick Marinos
Director, Cybersecurity and
Information Management Issues
United States Government Accountability Office
Washington, D.C. 20548

Dear Mr. Marinos:

Thank you for providing the U.S. Department of Education (Department or ED) with a draft copy of Government Accountability Office's (GAO) report, "FEDERAL STUDENT AID: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information" (GAO-18-121; Job Code 100500).

We appreciate the hard work that went into the audit and the opportunity to comment on the draft report. As Deputy Chief Operating Officer of Federal Student Aid (FSA), I am pleased to provide below the Department's responses to each of GAO's seven recommendations to the Secretary of Education.

Recommendation 1: The Secretary of Education should direct the Chief Operating Officer of FSA to establish and document a procedure for the destruction of records contained in electronic systems in accordance with approved disposition schedules.

Response: The Department partially concurs with this recommendation, as it believes FSA already has appropriate procedures in place. Although GAO's recommendation is based on sound principles, the draft report comingles the processes for the destruction of records that include structured data and unstructured data resulting in an inaccurate assessment of one process instead of two distinct processes. The draft report's failure to distinguish structured data and unstructured data limits the Department's ability to concur with this recommendation to the extent FSA already has in place two processes for the treatment of records with structured and unstructured data that comply with National Archives and Records Administration (NARA) regulations.

As established by NARA regulations in 36 CFR Part 12, the Department provides for disposition of electronic records that contain structured and unstructured data. Each type of data must be appropriately dispositioned (e.g., destroyed, archived, etc.).

Unstructured data is text-based documentation of FSA's activities that are preserved as federal records (such as standard operating procedures, program activities, etc.). These records are largely electronic files that are stored on shared drives. FSA will adhere to the Department's directed interim guidance for managing electronic format records until an Enterprise Electronic

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

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

Records Management System (EERMS) is available. The interim process is NARA compliant, documented in the Department's Records Management Directive and is similar to the paper record processes accurately outlined in the draft GAO report. Unstructured data records (documents) will be captured and preserved by the EERMS, when this new system is fully implemented.

Structured data, in contrast, is system-level data that are maintained and stored in a specific system/application and used for data processing of information, including for processing student loans. Structured data also must be managed and dispositioned. At FSA, this management occurs as part of the system lifecycle management methodology (LMM) process. Data are maintained until they meet the retention period and FSA has determined the data are no longer needed for any business or litigation purpose. FSA's documented LMM process ensures that data are not destroyed prematurely by establishing a record schedule at system initiation and through the operation of its Operations and Maintenance plan.

We respectfully note FSA has documented and implemented processes for both structured and unstructured data. The LMM process covers structured data systems from initiation, throughout system life, including change management, closing with systems' retirement. Similarly, FSA follows the Department's interim NARA compliant process to oversee and dispose of unstructured data in electronic records. Please note it is not a NARA violation to retain unstructured data longer than the assigned/approved schedule. However, as a result of this audit, the Department will conduct a review of FSA systems to assess if structured data are being retained beyond the scheduled destruction date calculation.

Recommendation 2: The Secretary of Education should direct the Chief Operating Officer of FSA to ensure staff receives records management training annually.

Response: The Department concurs with and has already implemented this recommendation to ensure FSA staff receives records management training annually. The Department completed its Fiscal Year 2017 (FY 17) mandatory records management training on September 30, 2017. The Department will continue to require annual records management training of its FSA staff.

Recommendation 3: The Secretary of Education should direct the Chief Operating Officer of FSA to conduct the triennial assessment of the FSA records management program.

Response: The Department concurs with and has already begun implementation of this recommendation to conduct the triennial assessment of the FSA records management program. We completed the data collection phase of the 2017 organization-wide internal records management self-assessment on September 30, 2017, and expect to complete the process by December 31, 2017.

Recommendation 4: The Secretary of Education should direct the Chief Operating Officer of FSA to ensure that privacy impact assessments address all required elements.

Response: The Department concurs with this recommendation to ensure that privacy impact assessments address all required elements and has already taken steps to implement a plan to address it.

In the GAO report, the evaluators found that "Policies for Protecting PII Generally Aligned with Federal Guidance, But Privacy Impact Assessments Did Not Consistently Address Key Elements." The evaluators noted that the Privacy Impact Assessments (PIAs) did not always contain all of the required elements and that some of the PIAs were not up to date. The Department's Office of the Chief Privacy Officer (OCPO) is responsible for coordinating the PIA process for the Department, including FSA. The Department's first PIA template, drafted in 2002, addressed the seven required elements found in the Office of Management and Budget (OMB) Memorandum OMB M-03-22. As OMB added more requirements, such as those found in OMB M-10-22 (for PIAs about third-party websites or applications), and as agencies were required to demonstrate compliance with NIST 800-53 Rev. 4, Appendix J and OMB Circular A-130, the Department updated its PIA template to ensure that these requirements were met. As systems that required a PIA changed, the system owners completed the PIAs in the updated templates. Therefore, PIAs completed prior to a new requirement would not address those required elements until a system change necessitated a new PIA.

Moreover, under the law, OMB policy, and ED policy there was no requirement to update the PIA except when substantive changes to the system occurred. Therefore, as long as there were no substantive changes to the system, there was no requirement that the PIA be updated. However, in September 2016, the OCPO published a policy specifically addressing the E-Gov Act, which included a requirement that "PIAs must be reviewed whenever a system change creates new privacy risks and at least every two (2) years, and updated if a system change creates new privacy risks or to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form." Since that policy was implemented, OCPO has reached out to all of ED's Principal Offices, including FSA, to ask that they review their systems and the associated PIAs, and to determine if an update is required. If so, OCPO asks that they update the PIA in the new template which includes all required elements. If not, the system owner can certify that the PIA is valid as written, and the date will be updated to show it is current. This is an ongoing and lengthy process, which is slowed by resource challenges. That said, FSA is continuing its work to update its PIAs, including the newly required elements.

Recommendation 5: The Secretary of Education should direct the Chief Operating Officer of FSA to ensure that information security-related policies and procedures are reviewed at least annually, in accordance with FSA policy; updated as needed; and approved by security officials.

Response: The Department concurs with this recommendation. Prior to the release of this report, during FY 17, FSA conducted an analysis of all information security related guidance on the official repository to identify items that needed to be updated. All active guidance documents were reviewed and, if required, updated, in FY 17. All expired guidance documents were officially retired from circulation. In the first quarter of FY 18, a second analysis will be conducted to ensure guidance documents requiring an update are added to the update calendar for FY 18. FSA will review its information security procedures and other FSA-specific

information security guidance documents. FSA and the Department will work together to conduct an annual review of their respective information security policies.

Recommendation 6: The Secretary of Education should incorporate into its program review process the review of postsecondary schools' information security program requirements.

Response: The Department agrees that FSA is responsible for monitoring and promoting school information security program requirements but believes that the annual compliance audit process is more appropriate, and will promote better consistency and implementation over time, than the program review process.

As noted in our response to recommendation 7, all participating postsecondary schools, as part of the program participation agreement with the Department, are required to certify that they are in compliance with the Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission (Safeguards Rule), as required by the Gramm-Leach-Bliley Act, P.L. 106-102 (GLBA). This certification provides the Department with the authority to oversee the schools' compliance with the requirement. One of the Department's primary oversight mechanisms for ensuring compliance with the requirements in the program participation agreement is the annual compliance audit that schools are required to have conducted by independent auditors under the GAO's government auditing standards. The Department is working with OMB and the Office of Inspector General (OIG) to update the guidance to ensure postsecondary schools' compliance with information security program requirements.

The independent compliance audit guidelines in the OMB Compliance Supplement and in the OIG audit guide do not include a requirement for the auditor to review schools' information security programs. The Department began the process of requesting an update to the OMB Compliance Supplement and the OIG audit guide in December 2016 and April 2017, respectively, to ensure schools' compliance with information security program requirements. Schools are required to submit compliance audits to the Department, and incorporating testing for the information security requirements into the audits will provide a consistent process for the Department to identify security weaknesses and require that schools implement corrective actions. The Department receives and resolves some compliance audits containing findings of security violations, but updating the OMB Compliance Supplement and OIG audit guide will significantly enhance consistent annual oversight of this area. Updating the OMB Compliance Supplement and OIG audit guide will take a few years to fully implement.

Thus, even before the audit process is in place, FSA staff will take follow-up actions when the information security program issues for a postsecondary school are identified during an FSA program review, either through program review staff observations or discussions with school staff. These follow-up actions will be similar to FSA's incident protocol response to a reported data breach, which response incorporates the GLBA checklist and the Safeguards Rule. FSA will update its program review process manual to reflect these procedures by no later than the date the final corrective action plan on this recommendation is due to GAO. In addition, as an interim measure until the audit review process is implemented, depending on the availability of resources and technical training, FSA will also consider including information security issues as

part of program reviews or other monitoring and oversight through the use of surveys or sampling.

As noted above, implementing compliance audit procedures will provide oversight at participating institutions. FSA's Program Compliance staff conducts program reviews at between 200 to 300 schools each year, and these reviews primarily focus on Title IV program requirements such as institutional and student eligibility, disbursement and return of Title IV aid and general recordkeeping. FSA has hired a person with the technical expertise to evaluate the issues and ensure appropriate corrective actions for security issues identified during these compliance audits. Auditors performing the annual compliance audit are required to have the expertise to perform the required audit procedures thereby ensuring more complete coverage than the Department could provide through program reviews, and putting in place specific security audit procedures will require the auditors to be qualified to conduct those audits.

GAO states that "given this lack of oversight, serious information security breaches have been allowed to occur." The Department does not agree that security breaches have been "allowed to occur." This implies that the Department was aware that conditions existed in these situations and did nothing to prevent such occurrences. This is not the case. When the Department becomes aware of a data breach, FSA has an incident protocol that is followed to address the incident, which includes contact with the school to ensure corrective actions are implemented to adequately protect the students and their data. The intent of the Department's work to request an update to the compliance supplement and audit guide is to identify any weaknesses that could potentially result in a breach and require the school to correct those weaknesses.

Recommendation 7: The Secretary of Education should update its regulation to include protections of personal information as an element of a school's ability to demonstrate its administrative capability.

Response: The Department does not concur with this recommendation regarding updating its regulation given existing statutory and regulatory provisions.

Pursuant to the Higher Education Act of 1965, in 20.U.S.C. 1094 (HEA), the regulation at 34 CFR § 668.16 states: "to begin and to continue to participate in any Title IV, HEA program, an institution shall demonstrate to the Secretary that the institution is capable of adequately administering that program under each of the standards established in this section. The Secretary considers an institution to have that administrative capability if the institution . . . establishes and maintains records required under this part and the individual Title IV, HEA program regulations…." Further, the Program Participation Agreement entered into by the Department and the school states: The institution agrees to comply with-- The Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission, as required by the Gramm-Leach-Bliley Act, P.L.106-102. These Standards are intended to ensure the security and confidentiality of customer records and information. The Secretary considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability as stated in 34 C.F.R. 668.16(c). Institutions are strongly encouraged to inform its students and the Department of any such breaches. The Department believes that the above two provisions provide the Department with sufficient authority to require schools to

protect personal information as an element of a school's ability to demonstrate its administrative capability.

I appreciate your examination of this important issue.

Sincerely

Matthew D. Sessa

Matthew D. Sessa
Deputy Chief Operating Officer

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, key contributors to this report were Anjalique Lawrence (Assistant Director), Elena Epps (Analyst in Charge), Gerard Aflague, James Ashley, Kami Brown, Christopher Businsky, Alan Daigle, Lisa Hardman, Paris Hawkins, Charles Hubbard, Lee McCracken, Carlo Mozo, David Plocher, Carl Ramirez, Minette Richardson, Kelly Rubin, Sukhjoot Singh, Priscilla Smith, Andrew Stavisky, Khristi Wilkins, and Robert Williams, Jr.

Appendix V: Accessible Data

Data Tables

Data Table for Figure 7: Population Estimates of National Archives and Records Administration's Required Records' Disposition Control Activities Used by Schools

Disposition Control Activity	Percentage
Regular review of records inventories	82
Monitor shredding services	65
Annual records clean out activities	63
Perform ad hoc monitoring of trash and recycle bins	45
Obtain pre-authorization before records are destroyed	45
Receive notifications when large trash bins or removal of boxes are requested	41
Approval process for disposal notices from off-site storage	36
Require certificates of destruction	32

Data Table Figure 8: Population Estimates of Federal Student Aid Record Storage Methods Used By Schools

Storage Method	Percentage
Locked filing cabinets on/off campus	90
Locked office on campus	84
Locked storage room on campus	77
Fireproof cabinets	63
School-owned records storage facility	46
Contractor-owned records storage facility	13

Agency Comment Letter

Text of Appendix III: Comments from the Office of Federal Student Aid, Department of Education

Page 1

Mr. Nick Marinos

Director, Cybersecurity and Information Management Issues

United States Government Accountability Office Washington, D.C. 20548

Dear Mr. Marinos:

Thank you for providing the U.S. Department of Education (Department or ED) with a draft copy of Government Accountability Office's (GAO) report, "FEDERAL STUDENT AID: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information" (GAO-18-121; Job Code 100500).

We appreciate the hard work that went into the audit and the opportunity to comment on the draft report. As Deputy Chief Operating Officer of Federal Student Aid (FSA), I am pleased to provide below the Department's responses to each of GAO's seven recommendations to the Secretary of Education.

Recommendation 1:

The Secretary of Education should direct the Chief Operating Officer of FSA to esta blish and document a procedure for the destruction of records contained in electronic systems in accordance with approved disposition schedules.

Response:

The Department partially concurs with this recommendation, as it believes FSA already has appropriate procedures in place. Although GAO's recommendation is based on sound principles, the draft report comingles the processes for the destruction of records that include structured data and unstructured data resulting in an inaccurate assessment of one process instead of two distinct processes. The draft report's failure to distinguish structured data and unstructured data limits the Department' s ability to concur with this recommendation to the extent FSA already has in place two processes for the treatment of records with structured and unstructured data that comply with National Archives and Records Administration (NARA) regulations.

As established by NARA regulations in 36 CFR Part 12, the Department provides for disposition of electronic records that contain structured and unstructured data. Each type of data must be appropriately dispositioned (e.g., destroyed, archived, etc.).

Unstructured data is text-based documentation of FSA's activities that are preserved as federal records (such as standard operating procedures, program activities, etc.). These records are largely electronic files that are stored on shared drives. FSA will adhere to the Department's directed interim guidance for managing electronic format records until an Enterprise Electronic

Page 2

Records Management System (EERMS) is available. The interim process is NARA compliant, documented in the Department's Records Management Directive and is similar to the paper record processes accurately outlined in the draft GAO report. Unstructured data records (documents) will be captured and preserved by the EERMS, when this new system is fully implemented.

Structured data, in contrast, is system-level data that are maintained and stored in a specific system/application and used for data processing of information, including for processing student loans. Structured data also must be managed and dispositioned. At FSA, this management occurs as part of the system lifecycle management methodology (LMM) process. Data are maintained until they meet the retention period and FSA has determined the data are no longer needed for any business or litigation purpose. FSA' s documented LMM process ensures that data are not destroyed prematurely by establishing a record schedule at system initiation and through the operation of its Operations and Maintenance plan.

We respectfully note FSA has documented and implemented processes for both structured and unstructured data. The LMM process covers structured data systems from initiation, throughout system life, including change management, closing with systems' retirement. Similarly, FSA follows the Department's interim NARA compliant process to oversee and dispose of unstructured data in electronic records. Please note it is not a NARA violation to retain unstructured data longer than the assigned/approved schedule. However, as a result of this audit, the Department will conduct a review of FSA systems to assess if structured data are being retained beyond the scheduled destruction date calculation.

Recommendation 2:

The Secretary of Education should direct the Chief Operating Officer of FSA to ensure staff receives records management training annually.

Response:

The Department concurs with and has already implemented this recommendation to ensure FSA staff receives records management training annually. The Department completed its Fiscal Year 2017 (FY 17) mandatory records management training on September 30, 2017. The Department will continue to require annual records management training of its FSA staff.

Recommendation 3:

The Secretary of Education should direct the Chief Operating Officer of FSA to conduct the triennial assessment of the FSA records management program.

Response:

The Department concurs with and has already begun implementation of this recommendation to conduct the triennial assessment of the FSA records management program. We completed the data collection phase of the 2017 organization-wide internal records management self-assessment on September 30, 2017, and expect to complete the process by December 31, 2017.

Recommendation 4:

The Secretary of Education should direct the Chief Operating Officer of FSA to ensure that privacy impact assessments address all required elements.

Page 3

Response:

The Department concurs with this recommendation to ensure that privacy impact assessments address all required elements and has already taken steps to implement a plan to address it.

In the GAO report, the evaluators found that "Policies for Protecting PII Generally Aligned with Federal Guidance, But Privacy Impact Assessments Did Not Consistently Address Key Elements." The evaluators noted that the Privacy Impact Assessments (PIAs) did not always contain all of the required elements and that some of the PIAs were not up to date. The Department's Office of the Chief Privacy Officer (OCPO) is responsible for coordinating the PIA process for the Department, including FSA. The Department's first PIA template, drafted in 2002, addressed the seven required elements found in the Office of Management and Budget (0MB) Memorandum 0MB M-03-22. As 0MB added more requirements, such as those found in 0MB M-10-22 (for PIAs about third-party websites or applications), and as agencies were required to demonstrate compliance with NIST 800-53 Rev. 4, Appendix J and 0MB Circular A- l 30, the Department updated its PIA template to ensure that these requirements were met. As systems that required a PIA changed, the system owners completed the PIAs in the updated templates. Therefore, PIAs completed prior to a new requirement would not address those required elements until a system change necessitated a new PIA.

Moreover, under the law, 0MB policy, and ED policy there was no requirement to update the PIA except when substantive changes to the system occurred. Therefore, as long as there were no substantive changes to the system, there was no requirement that the PIA be updated.

However, in September 2016, the OCPO published a policy specifically addressing the E-Gov Act, which included a requirement that " PIAs must be reviewed whenever a system change creates new privacy risks and at least every two (2) years, and updated if a system change creates new privacy risks or to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form." Since that policy was implemented, OCPO has reached out to all of ED's Principal Offices, including FSA, to ask that they review their systems and the associated PIAs, and to determine if an update is required. If so, OCPO asks that they update the PIA in the new template which includes all required elements. If not, the system owner can certify that the PIA is valid as written, and the date will be updated to show it is current. This is an ongoing and lengthy process, which is slowed by resource challenges. That said, FSA is continuing its work to update its PIAs, including the newly required elements.

Recommendation 5:

The Secretary of Education should direct the Chief Operating Officer of FSA to ensure that information security-related policies and procedures are reviewed at least annually, in accordance with FSA policy; updated as needed; and approved by security officials.

Response:

The Department concurs with this recommendation. Prior to the release of this report, during FY 17, FSA conducted an analysis of all information security related guidance on the official repository to identify items that needed to be updated. All active guidance documents were reviewed and, if required, updated, in FY 17. All expired guidance documents were officially retired from circulation. In the first quarter of FY 18, a second analysis will be conducted to ensure guidance documents requiring an update are added to the update calendar for FY 18. FSA will review its information security procedures and other FSA-specific

Page 4

information security guidance documents. FSA and the Department will work together to conduct an annual review of their respective information security policies.

Recommendation 6:

The Secretary of Education should incorporate into its program review process the review of postsecondary schools' information security program requirements.

Response:

The Department agrees that FSA is responsible for monitoring and promoting school information security program requirements but believes that the annual compliance audit process is more appropriate, and will promote better consistency and implementation over time, than the program review process.

As noted in our response to recommendation 7, all participating postsecondary schools, as part of the program participation agreement with the Department, are required to certify that they are in compliance with the Standards for Safeguarding Customer Information , 16 C.F.R.

Part 314, issued by the Federal Trade Commission (Safeguards Rule), as required by the Gramm-Leach- Bliley Act, P.L. 106-102 (GLBA). This certification provides the Department with the authority to oversee the schools' compliance with the requirement. One of the Department' s primary oversight mechanisms for ensuring compliance with the requirements in the program participation agreement is the annual compliance audit that schools are required to have conducted by independent auditors under the GAO's government auditing standards. The Department is working with 0MB and the Office oflnspector General (OIG) to update the guidance to ensure postsecondary schools' compliance with information security program requirements.

The independent compliance audit guidelines in the 0MB Compliance Supplement and in the OIG audit guide do not include a requirement for the auditor to review schools' information security programs. The Department began the process of requesting an update to the 0MB Compliance Supplement and the OIG audit guide in December 2016 and April 2017, respectively, to ensure schools' compliance with information security program requirements. Schools are required to submit compliance audits to the Department, and incorporating testing for the information security requirements into the audits will provide a consistent process for the Department to identify security weaknesses and require that schools implement corrective actions. The Department receives and resolves some compliance audits containing findings of security violations, but updating the 0MB Compliance Supplement and OIG audit guide will significantly enhance consistent annual oversight of this area. Updating the 0MB Compliance Supplement and OIG audit guide will take a few years to fully implement.

Thus, even before the audit process is in place, FSA staff will take follow-up actions when the information security program issues for a postsecondary school are identified during an FSA program review, either through program review staff observations or discussions with school staff. These follow-up actions will be similar to FSA's incident protocol response to a reported data breach, which response incorporates the GLBA checklist and the Safeguards Rule. FSA will update its program review process manual to reflect these procedures by no later than the date the final corrective action plan on this recommendation is due to GAO. In addition, as an interim measure until the audit review process is implemented, depending on the availability of resources and technical training, FSA will also consider including information security issues as

Page 5

part of program reviews or other monitoring and oversight through the use of surveys or sampling.

As noted above, implementing compliance audit procedures will provide oversight at participating institutions. FSA's Program Compliance staff conducts program reviews at between 200 to 300 schools each year, and these reviews primarily focus on Title IV program requirements such as institutional and student eligibility, disbursement and return of Title IV aid and general recordkeeping. FSA has hired a person with the technical expertise to evaluate the issues and ensure appropriate corrective actions for security issues identified during these compliance audits. Auditors performing the annual compliance audit are required to have the expertise to perform the required audit procedures thereby ensuring more complete coverage than the Department could provide through program reviews, and putting in place specific security audit procedures will require the auditors to be qualified to conduct those audits.

GAO states that "given this lack of oversight, serious information security breaches have been allowed to occur." The Department does not agree that security breaches have been "allowed to occur." This implies that the Department was aware that conditions existed in these situations and did nothing to prevent such occurrences. This is not the case. When the Department becomes aware of a data breach, FSA has an incident protocol that is followed to address the incident, which includes contact with the school to ensure corrective actions are implemented to adequately protect the students and their data. The intent of the Department' s work to request an update to the compliance supplement and audit guide is to identify any weaknesses that could potentially result in a breach and require the school to correct those weaknesses.

Recommendation 7:

The Secretary of Education should update its regulation to include protections of personal information as an element of a school's ability to demonstrate its administrative capability.

Response:

The Department does not concur with this recommendation regarding updating its regulation given existing statutory and regulatory provisions.

Pursuant to the Higher Education Act of 1965, in 20.U.S.C. 1094 (HEA), the regulation at 34 CFR § 668.16 states: "to begin and to continue to participate in any Title IV, HEA program, an institution shall demonstrate to the Secretary that the institution is capable of adequately administering that program under each of the standards established in this section. The Secretary considers an institution to have that administrative capability if the institution ... establishes and maintains records required under this part and the individual Title IV, HEA program regulations...." Further, the Program Participation Agreement entered into by the Department and the school states: The institution agrees to comply with-- The Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission, as required by the Gramm-Leach-Bliley Act, P.L.106-102. These Standards are intended to ensure the security and confidentiality of customer records and information. The Secretary considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability as stated in 34 C.F.R. 668.16(c). Institutions are strongly encouraged to inform its students and the Department of any such breaches. The Department believes that the above two provisions provide the Department with sufficient authority to require schools to

Page 6

protect personal information as an element of a school's ability to demonstrate its administrative capability.

I appreciate your examination of this important issue.

Sincerely

Matthew D. Sessa

Deputy Chief Operating Officer

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548