September 2018

CYBERSECURITY

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

GAO Highlights

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

Why GAO Did This Study

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

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

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

What GAO Recommends

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

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

What GAO Found

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

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

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

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

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

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

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

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

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