FINAL MANAGEMENT INFORMATION REPORT

DATE: September 30, 2013

TO: James W. Runcie
Chief Operating Officer
Federal Student Aid

FROM: Charles E. Coe, Jr. //s//
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations

SUBJECT: Final Management Information Report
PIN Security Vulnerabilities
Control No. ED-OIG/X21L0002 (12-110380)

The purpose of this Management Information Report is to inform Federal Student Aid (FSA) of our concerns about security vulnerabilities associated with the Personal Identification Number (PIN) Registration System (PIN system) that the Office of Inspector General (OIG) has identified through various investigations and to make recommendations and suggestions for addressing these vulnerabilities.

In preparing this report, the OIG reviewed FSA's response to the recommendation in the OIG Investigative Program Advisory Report (IPAR) *Distance Education Fraud Rings* (L42L0001)(September 26, 2011) regarding the PIN system.[1] We also reviewed an FSA PowerPoint outlining a general plan to replace the PIN system, although it did not identify any identity verification and electronic authentication controls to address security vulnerabilities.[2] This Management Information Report recommends changes to the current PIN system and recommends controls FSA should incorporate into the replacement system to address PIN recovery mechanism vulnerabilities. This report also provides suggestions to limit the risks associated with students using third parties in the student financial assistance process.

The OIG learned from FSA's September 16, 2013, response to our draft of this report that FSA is in the process of re-engineering and replacing the PIN system with the Non-privileged Access

[1] The *Distance Education Fraud Rings* IPAR alerted FSA and the Office of Postsecondary Education of the OIG's findings from investigations of fraud involving distance education programs and made recommendations to mitigate the risk of fraud in such programs. The IPAR recommended that the Department implement controls in the PIN delivery system to identify and prevent the issuance of multiple PINs to the same email address without confirmation of identity.

[2] Identity verification (also known as identity "proofing") is when a person's identity is verified for the purpose of issuing information system credentials. Electronic authentication is the process of establishing confidence in the user identity through the use of information system credentials.

System (NPAS), which FSA stated will solve the problems that we have identified in our report and will provide additional security improvements. FSA has not provided the OIG with any supporting documentation related to NPAS beyond what was explained in FSA's response to our draft report; nor has it finalized the contract for the development of NPAS. The OIG has not validated FSA's plans for NPAS.

In addition, FSA did not agree with our suggestion to enable students to permit companies providing loan-related services read-only access to relevant areas of their accounts that do not contain sensitive personal information. FSA stated that the deployment of the MyStudentData Download permits students to download a file that includes their loan and grant information and provide that to third parties if they choose. However, we do not know whether MyStudentData Download will reduce the incidence of PIN sharing in light of its limitations, but we believe that allowing third parties limited, read-only access to student accounts would reduce the problem of PIN sharing and unfettered third party access to personal data.

FSA did not agree with our suggestion to consider creating preparer-specific access accounts that would allow a student to authorize a preparer to access and modify certain sections of the FAFSA because it considers such access to an applicant's file/data would compromise the integrity of the Title IV student aid application process. According to FSA, the extensive "smart-logic" of the FAFSA on the Web product maintains the applicant's control of their personal data and FAFSA submissions, and MyStudentData Download provides sufficient third party access needed for counseling and other advisory activities. We do not believe that MyStudentData Download will reduce this problem because it does not provide data that assists third parties who help students complete their applications. In addition, the OIG does not know how "smart logic," in which FAFSA on the Web skips over questions that do not apply to the student or prompts the student for customized follow-up questions, will prevent a student who has already chosen to use a preparer from sharing their PIN with the preparer or allowing the preparer to manage the student's account.

BACKGROUND

Personal Identification Number

The FSA PIN is a four-digit number that is used in combination with the user's Social Security number (SSN), name, and date of birth (DOB). The PIN serves as an electronic signature and provides access to sensitive personal records on FSA Web sites such as fafsa.ed.gov and pin.ed.gov. The PIN allows students and their parents the ability to manage their FSA accounts, manage their Free Application for Federal Student Aid (FAFSA), and electronically sign the FAFSA and other related documents. FSA requires each person accessing these sites to apply for his or her own PIN. FSA is responsible for securing and maintaining the PIN and FAFSA Web sites, applications, and transactions.

Sensitive Personal Information Stored in FSA Documents and Web Sites

As part of the process of applying for a PIN or completing the FAFSA, users provide personally identifiable and financial information. The PIN application collects and contains sensitive personal information including name, SSN, DOB, email address, physical address, challenge question, and challenge answer.

The Student Aid Report, which a user may access using a PIN, contains sensitive personal information that was provided on the FAFSA such as name, SSN, DOB, email address, permanent address, sensitive financial and income information, marital status, high school, choice of post-secondary school, personal identifiers for parents and step-parents, and financial information and marital status for parents and step-parents.

During a person's FAFSA and PIN application process, (b)(7)(E) (b)(7)(E) The Central Processing System selects certain FAFSA applicants who must verify their identity and certify that they will use their financial aid for educational purposes.[4] (b)(7)(E) (b)(7)(E)

FSA's Plans for the PIN Replacement System

In response to the OIG's *Distance Education Fraud Rings* IPAR, FSA documented PIN vulnerabilities in a PowerPoint entitled, "Shared Use of the PIN," dated June 21, 2012. (b)(7)(E) (b)(7)(E)

In April 2013, the OIG requested that the FSA Information System Security Officer provide us with an update on FSA's planned electronic verification and identity verification controls to address vulnerabilities identified in the OIG's *Distance Education Fraud Rings* IPAR and FSA's PowerPoint on "Shared Use of the PIN."

The FSA Information System Security Officer stated that FSA has been researching an internally developed solution for the PIN replacement system and was planning to create a single sign-on solution for all FSA Web sites.[5] FSA provided us a PowerPoint regarding the plans for the PIN replacement system.[6] The PowerPoint stated that the replacement system will help modernize the process of assigning a PIN to eligible non-privileged users (borrowers), streamline authentication for the systems that non-privileged users access, and decrease the security and compliance risks associated with using personally identifiable information for access to FSA systems. However, the PowerPoint did not describe specific identity verification or electronic authentication controls for non-privileged user access to FSA systems.

We last requested specific information on the planned controls FSA will include in the PIN replacement system in May 2013, but FSA did not provide us this information at that time or since then. In its response to our draft report, FSA described how the planned NPAS system will

[3] The Central Processing System is the automated system that processes all applications for Federal student aid, calculates financial aid eligibility, and notifies students and educational institutions of the results of the eligibility calculation.

[4] The student accomplishes this verification by presenting identification to a notary public or school official and signing an Identity and Statement of Education Purpose.

[5] A single sign-on will allow users to access all FSA websites with one user ID and password.

[6] The PowerPoint is entitled, "PIN Re-engineering and Replacement (Enterprise Identity Management Services (EIMS) Phase 2)."

address our recommendations. We reviewed the explanation FSA included in its response to our draft report, but have not received supporting documentation related to the plan and FSA has not yet finalized a contract for the development of the system.

PIN RECOVERY MECHANISM NOT ADEQUATE

A March 2004 OIG audit of the *Implementation of Electronic Signatures for Select Federal Student Aid Transactions* (ED-OIG A11D0002) (b)(7)(E) Since this audit was issued, the OIG has investigated several cases of unauthorized access to sensitive personal information contained in the PIN system and found that vulnerabilities continue to exist in the PIN system.

(b)(7)(E)

Guidance and Best Practices on Authentication and Password Management

Since 2001, the Federal government and financial institutions have issued the following guidance and best practices on authentication and password management:

- If the user does not supply challenge questions but rather selects questions from a list provided by the registration site, the user should select from a set of at least five questions and be required to answer three questions to authenticate.[8]
- Sophisticated challenge questions provide better security. Examples include answering questions that require specific user knowledge (such as the exact amount of the user's monthly mortgage payment, selecting a familiar address from a list of addresses, or identifying a user-selected image from several images).[9]
- Adding a "Last Login" feature to display a user's last login and number of failed login attempts each time they successfully log in; if the last login date and time displayed does not coincide with the date and time that the user last logged into his/her account, the user will be alerted to a possible compromise of his or her PIN.[10]

[7] The PIN account includes information such as the account holder's email address, phone number, and mailing address.
[8] National Institute of Standards and Technology (NIST), Special Publication (SP) 800-63-1, "Electronic Authentication Guideline," (Dec. 2011).
[9] FIL-50-2011 and Federal Financial Institutions Examination Council, "Supplement to Authentication in an Internet Banking Environment," (October 2005).
[10] National Institute of Standards and Technology, Special Publication 800-63-1.

- Using "out-of-band authentication," which is a process to authenticate the identity of the person originating a transaction through a channel different from the one that person used to initiate the transaction. Methods of out-of-band authentication include sending the user an email or text message that has information they must use to log in.[11]

(b)(7)(E)

PIN Recovery Mechanism Can Be Exploited

(b)(7)(E)

(b)(7)(E)

(b)(7)(E) The challenge questions range in distinctiveness and in how easy or difficult the answers would be for an unauthorized user to guess. The three most popular challenge questions are listed in the table below.

Table: Three Most Popular PIN Challenge Questions

PIN Challenge Question	Percentage of People Choosing This Question
What is your mother's maiden name?	30%
What city were you born in?	29%
What is your favorite color?	13%

Unauthorized User Can (b)(7)(E)

The OIG is investigating a case where an unauthorized user gained control of another user's PIN

(b)(7)(E)

(b)(7)(E)

[11] Federal Financial Institutions Examination Council, "Supplement to Authentication in an Internet Banking Environment," (October 2005).

Impact
(b)(7)(E)

After obtaining a person's PIN, an unauthorized user can view or change the owner's personal information on the PIN Web site. In addition, an unauthorized user can use the PIN on the FAFSA Web site to view the student's sensitive personal information contained in the Student Aid Report or to submit a new (b)(7)(E)

Unauthorized access may leave the PIN owner susceptible to loss of financial aid, unwanted contact, potential financial harm due to the disclosure of sensitive information, or other harmful activities.

RECOMMENDATIONS

The OIG recommends that FSA implement the following improvements to the PIN recovery mechanism to ensure personal information stored on FSA Web sites is adequately protected:

(b)(7)(E)

FSA Response

In response to our recommendations, FSA stated:

(b)(7)(E)

(b)(7)(E)

5. FSA will research and consider the OIG-provided options for (b)(7)(E)

OIG Response

It appears that FSA's planned actions for recommendations 1, 2, 3, and 5 will address the vulnerabilities identified in this report. We found FSA's response to recommendation 4 partially non-responsive because it only addresses new accounts and not re-enabled accounts. (b)(7)(E)
(b)(7)(E)

During the course of our review, we requested specific information on the controls planned for the PIN replacement system, which we noted in the Draft Management Information Report provided to FSA on August 27, 2013. Because we just learned about NPAS in FSA's September 16, 2013, response to our draft report and FSA did not provide supporting documentation beyond what was explained in its response to our draft report, we have not validated FSA's plan for NPAS implementation.

COMPANIES THAT REQUIRE PINs TO ACCESS FSA SYSTEMS

An OIG investigation found that students sharing their PINs with an Internet-based company providing loan-related services to the students provided an opportunity for bad actors at the company to change and misuse the students' personal data. As a result of this investigation, the OIG researched this and other Internet-based companies that log into FSA systems using students' PINs. We found that students using the services of these companies type their PIN into the company's Web site so the company can obtain information on the student's behalf.[12] Using this data, companies may help students understand and manage debt and provide information and assistance about loan repayment or consolidation options. The OIG is reporting our research regarding these companies to inform you of additional facts to consider when establishing and implementing requirements for the single sign-on solution for FSA Web sites.

FSA's Web site states, "Your PIN is used to sign legally binding documents electronically. It has the same legal status as a written signature. Don't give your PIN to anyone—not even to someone helping you fill out the FAFSA." The PIN Web site states, "If you receive a PIN, you

[12] In October 2012, the White House and the Department hosted an "Education Datapalooza" that included a discussion of the "MyData Initiative," a collaboration between the Department and software developers to create a simple mechanism for students to download their educational data, such as FAFSA data, to a provider's Web site. See FSA's "MyData Initiative" Web site.

agree not to share it with anyone. Your PIN serves as your electronic signature and provides access to your personal records, so you should never give your PIN to anyone, including commercial services that offer to help you complete your FAFSA. Be sure to keep your PIN in a safe place."

Although these Web sites state that the PIN should not be given to "anyone," it is possible that users may not consider the prohibition against sharing a PIN to encompass when a student inputs the PIN into a company's Web site so that it can retrieve data for the student. Given the Administration's efforts to help Americans manage their student loan debt, FSA may consider this type of service to be potentially beneficial to students; however, as mentioned above, sharing the PIN presents a possibility that the student will be exploited.

The OIG suggests that FSA consider developing a capability to enable students to permit companies providing loan-related services read-only access to relevant areas of their accounts that do not contain sensitive personal information. This would allow a student to grant these companies access to the student's loan-related information without the risk that a bad actor at the company could alter the student's record or obtain the student's sensitive personal information.

FSA Response

FSA did not agree with the OIG's suggestion but said that MyStudentData Download meets the OIG's objectives for this suggestion. The deployment of MyStudentData Download in November 2012 and April 2013 permits students to download a file that includes loan and grant information and provide that to third parties if they choose. FSA stated that it believes there is no reason to allow any party, other than the student, to have direct access (read-only or otherwise) to the student's FSA information.

OIG Response

MyStudentData Download only provides a snapshot at a given point in time versus the constant, real-time access that third parties have when students provide them their PINs. We do not know whether MyStudentData will reduce the incidence of PIN sharing in light of its limitations, but we believe that allowing third parties limited, read-only access to student accounts would reduce the problem of PIN sharing and unfettered third party access to personal data.

FAFSA PREPARERS MANAGING STUDENT PINs

The OIG previously reported in the *Distance Education Fraud Rings* IPAR that the Department does not verify that the user submitting a PIN request is the actual holder of the SSN. The IPAR also noted that single email addresses were used to receive and manage PIN accounts for sometimes hundreds of individuals. In response to these findings, FSA analyzed PIN security vulnerabilities and noted that the PIN is prone to abuse by third parties supposedly operating on behalf of financial aid recipients.

One such type of third party is FAFSA preparers. The OIG has found that between school years 2008-2009 and 2011-2012, four percent of FAFSA applicants listed a preparer on their FAFSAs. FAFSA applicants are not required to pay a fee to apply for Federal student aid. However, the Higher Education Act of 1965, as amended (HEA), authorizes an applicant for Federal student

aid to use a paid preparer for consultative or preparation services for completing the FAFSA. Only a preparer who is paid a fee is subject to the HEA's requirements; others who assist an applicant without charging a fee (e.g., guidance counselor, teacher, etc.) are not "preparers" within the meaning of the HEA. Section 483(d)(2) of the HEA provides that when a preparer submits a FAFSA to the Department, the preparer must include on the FAFSA their name, address or employer's address, SSN or Employer Identification Number (EIN), and organizational affiliation.

During an OIG proactive investigative project, we reviewed 6 preparer organizations that helped at least 435 students apply to college, file their FAFSAs, and manage their student loans. The OIG found these student PIN accounts were managed using an email address owned by the preparer organization and (b)(7)(E) [redacted]

The preparer organizations' respective Web sites indicated that, for a fee, they provide services such as applying for scholarships and grants, obtaining PINs, completing the FAFSA, managing student loans, and completing university-specific financial paperwork.[13]

The OIG noted the following for the 435 applicants:

- 86 percent of the FAFSA or PIN applications were submitted from the same Internet Protocol address as that of the preparer organization.
- 80 percent of PIN applications showed the same PIN challenge question and 78 percent chose the same challenge answer or established a challenge answer of: (b)(7)(E) [redacted]
- 99 percent of the FAFSA applicants associated with one particular preparer organization listed the preparer organization's email address as the student's personal email address. The majority of applicants associated with the other preparer organizations listed what appeared to be the student's personal email address or did not list any email address on the FAFSA.
- 97 percent of the FAFSA applications did not list the preparer's name, EIN, or SSN. If preparer organizations were paid for their services, those omissions violated the HEA.

Thus, preparer organizations may be submitting applications on behalf of students without identifying themselves on the FAFSA, controlling student PIN accounts, and receiving electronic correspondence from FSA that is intended for the student.

For these 435 applicants,[14] the OIG suggests that FSA require the students to change their PINs and reaffirm their agreements not to share their PINs with anyone, as well as verify the contact information in both the PIN system and the current year FAFSA with the student. The OIG also

[13] The OIG did not obtain student records maintained by the preparer organizations and therefore did not confirm whether students paid the preparer organizations. The OIG also did not determine if the preparer organization established the PIN or if the student provided their PIN to the preparer organization, which then changed the PIN to the last four digits of the student's SSN.
[14] The OIG will provide the list of students to FSA upon request.

suggests FSA consider controls that would ensure preparers are identifying themselves on the FAFSA.

To reduce the temptation for students to share their PIN with preparers, the OIG suggests FSA consider creating preparer-specific access accounts that would allow a student to authorize a preparer to access and modify certain sections of the FAFSA. FSA could set permissions that would prevent preparer-specific accounts from viewing or changing the student's sensitive personal information, email address, or postal address; signing the FAFSA for the student/parent; or submitting the FAFSA. If FSA created this type of account, it could also be used to automatically link a preparer's SSN or EIN to the submitted FAFSA. FSA could also present students a message, prior to students granting the preparer access to their FAFSA, reminding them that free assistance is available for completing and submitting a FAFSA. This may encourage some students to seek the free assistance rather than paying a company to assist them.

FSA Response

FSA did not agree with the OIG's suggestion and asserted that allowing third parties limited access to an applicant's file/data would compromise the integrity of the student aid application process and be contrary to the intent of the HEA. According to FSA, the extensive "smart-logic" of the FAFSA on the Web product maintains the applicant's control of their personal data and FAFSA submissions, and MyStudentData Download provides sufficient third party access needed for counseling and other advisory activities.

OIG Response

Our work has demonstrated that many students have disregarded the prohibition on sharing PINs and have provided third parties full access to their accounts, including access to their personal data. We do not believe that MyStudentData Download will reduce this problem because it does not provide data that assists third parties who help students complete their applications. In addition, the OIG does not know how "smart logic," in which FAFSA on the Web skips over questions that do not apply to the student or prompts the student for customized follow-up questions, will prevent a student who has already chosen to use a preparer from sharing their PIN with the preparer or allowing the preparer to manage the student's account. The OIG can provide FSA with a list of preparer email addresses found in PIN and FAFSA applications to further demonstrate the extent of the problem of third party access to student accounts. Indeed, the OIG re-checked student PIN accounts on September 25, 2013, and preparer email addresses were still listed on most accounts identified from our work.

OBJECTIVE, SCOPE, AND METHODOLOGY

The OIG recently investigated several cases of unauthorized access to personal information contained in the PIN Registration System and the FAFSA Web site. The unauthorized users in these cases were familiar with the student victim and included former spouses, estranged parents, and step-parents. The OIG is also investigating a case where an unauthorized user locked a victim's PIN account by submitting three incorrect challenge answers, applied for a new PIN using the victim's personal information, and submitted a fraudulent FAFSA using the victim's personal identifiers.

On January 31, 2011, the OIG started a proactive investigative project to identify behavior associated with fraud rings and identified suspicious trends related to student PINs and FAFSA preparers that occurred between academic years 2008-2009 and 2011-2012. The scope of this proactive investigative project covered a limited dataset where we analyzed specific behavior for potential referral to Investigation Services.

As a result of an investigation, the OIG researched Internet-based companies that obtain student data by logging into FSA systems using the student's PIN.

The OIG provided a draft of this report to FSA on August 27, 2013. FSA provided its response to the draft report, which was dated September 16, 2013. We are including FSA's response as an attachment to this report.

We conducted our work in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Inspection and Evaluation*.

If you have any questions, please contact Mark A. Smith, Special Agent in Charge, Technology Crimes Division, at (202) 245-7019.

cc: Dawn Dawson, Audit Liaison for FSA

UNITED STATES DEPARTMENT OF EDUCATION
Federal Student Aid

MEMORANDUM

DATE: September 16, 2013

TO: Charles E. Coe, Jr.
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations
Office of Inspector General

FROM: James W. Runcie
Chief Operating Officer

SUBJECT: Draft Management Information Report
PIN Security Vulnerabilities
Control No. ED-OIG/X21L0002 (12-110380)

Thank you for providing us with an opportunity to respond to the Office of Inspector General's (OIG) draft Management Information Report entitled, "PIN Security Vulnerabilities." Your report states that OIG reviewed Federal Student Aid's (FSA) responses to the recommendations in the OIG Investigative Program Advisory Report (IPAR) Distance Education Fraud Rings (L42L0001) dated September 26, 2011 regarding the (Personal Identification Number) PIN system and FSA's plans to replace the current PIN system.

We are pleased to have this opportunity to share the latest update on this project. FSA is in the process of re-engineering and replacing PIN with a new system, the Non-privileged Access System (NPAS). NPAS provides an identity and access management solution, based on industry best practices, that is adaptable to a changing business environment, while enabling improvements in security and customer usability. In addition, consistent with OIG recommendations, this solution will solve the problems your office identified and provide additional security improvements.

The NPAS is part of the Enterprise Identity Management Solution (EIMS) initiative. The EIMS objective is to "make provisioning and access management for FSA systems more efficient and secure for both privileged users (FSA and its partners) and non-privileged users (students/borrowers) through the implementation of enterprise Identity Lifecycle Management processes and technologies." EIMS is an umbrella initiative with several strategically related projects focused on achieving the EIMS objective.

In order to effectively develop NPAS, FSA collected and consolidated requirements from various stakeholders, including OIG's past recommendations. For the last year, FSA focused on

the planning, preparation and acquisition of NPAS, including the procurement for the services to development and implement the new system.

The new system will provide authorized FSA non-privileged external users a better and more secure capability for accessing FSA systems and data that:

- Does not require use of personal identification information (PII) during the login process and also provides these users the full range of identity and access management services, e.g., account creation; user provisioning and access; user self-care and other common capabilities; is able to effectively exchange data with other external and internal FSA systems for authentication and other purposes.
- Is able to readily support future functionality enhancements such as eSignature appliances; use of soft tokens, biometrics and other factors.
- Incorporates the use of strong and proven access controls, encryption, secure transmissions, and other technology advances, so all users are provided end-to-end protection of data, from entry source; while traversing the internet or intranets; and within data storage repositories.

Additionally, the new system will also comply with the broader FSA Information Technology standards, which require that the system:

- Provide evidence (e.g., National Institute of Standards and Technology (NIST) certificate for the specific product and module) that the products it utilizes provide cryptographic protections using modules that comply with Federal Information Processing Standards (FIPS) PUB 140-2 standards.
- Comply with the controls for access management contained in the current versions and revisions of: NIST SP-800-53, Recommended Security Controls for Federal Information Systems and Organizations; and NIST-SP-800-53A, Guide for Assessing Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans.
- Comply with the security authorization processes, as outlined in NISTSpecial Publication NIST-SP-800-37, entitled Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, and supporting Office of Chief Information Officer (OCIO) policies, standards, and procedures. In accordance with the identified risk rating, the solution shall satisfy the appropriate security controls as defined in FIPS 200 and NIST-SP 800-53, entitled "Recommended Security Controls for Federal Information Systems and Organizations."

As part of the planning process and as part of the PIN re-engineering, five Technical Proofs of Concept (TPOCs) were conducted as a cost effective means to test feasibility and scalability of proposed architecture and functionality. The TPOCs demonstrated that: (1) scaling up the existing infrastructure for over 100 million users is viable; (2) forms based authentication is feasible for legacy systems; (3) Federated Identity Management can be implemented; (4) integration with a commercial eSignature appliance is possible and (5) it is feasible to seamlessly integrate with legacy applications.

The current focus of the EIMS initiative is to complete the acquisition and finalize a contract for PIN Re-engineering and Replacement by late September 2013. Once the award is made, the vendor and the FSA Integrated Project Team will begin the re-engineering and replacement of PIN with two to three months of requirements definition, refinement and validation.

The following responds to each of your specific recommendations.

OIG Recommendation

1. Require PIN owners to (b)(7)(E)

FSA Response

The new system will require (b)(7)(E)

OIG Recommendation

2. Provide (b)(7)(E)

FSA Response

As noted above, the new system includes (b)(7)(E)

We are sensitive to the fact that inquiries regarding PINs, passwords and forgotten challenge responses are typically among the highest trending questions at the Federal Student Aid Information Center (FSAIC).

OIG Recommendation

3. Notify PIN owners of (b)(7)(E) In addition, ensure that (b)(7)(E)

FSA Response

(b)(7)(E)

OIG Recommendation

4. (b)(7)(E) [redacted]

FSA Response

[redacted] (b)(7)(E) [redacted]

(b)(7)(E) [redacted]

OIG Recommendation

5. Research and consider (b)(7)(E) [redacted] when PIN and FAFSA accounts are initially established.

FSA Response

FSA will research and consider other options, such as those listed above.

In addition to the formal recommendations, we will also address other suggestions contained in the draft report.

OIG Suggestion

The OIG suggests that FSA consider developing a capability to enable students to permit companies providing loan-related services read-only access to relevant areas of their accounts that do not contain sensitive personal information.

FSA Response

FSA does not agree with the OIG's suggestion. In November 2012 and April 2013, FSA deployed "MyStudentData Download" functionality for the National Student Loan Data System (NSLDS) and the FAFSA, respectively. These capabilities were developed in support of the White House Office of Science and Technology Policy's initiative, which strives to make education-related data available, machine-readable, and accessible while protecting the privacy of the student's personal information. A goal of the initiative is to empower students to electronically obtain, store, and if they so decide, to share their information with others while safeguarding personally identifiable information.

For NSLDS, the student can, with one simple action, download a simple text file that includes the student's Title IV loan and grant information (e.g., award amounts, disbursement amounts and dates). For FAFSA information, students are able to download their processed FAFSA data.

For both applications, the student may choose to share the downloaded information with third parties that provide assistance with various higher education decisions (e.g., how to pay for an education, and how to manage debt if they use loans to fund their education.) Since the information provided by the student to a third party is not directly from the FSA system that maintains the data, the third party does not have access to those systems and cannot change or update any of the information. Those capabilities remain solely with the student.

The file layouts for the FAFSA and NSLDS downloads are included in the e-announcement below. The layouts/data elements were approved by Office of the General Counsel prior to implementation.

http://ifap.ed.gov/eannouncements/111312UpcomingMyStudentDataDownloadFunction1314FOTWDraftFileLayout.html

http://ifap.ed.gov/eannouncements/081612MyDataButtonUpcomingImplementation.html

In summary, FSA believes that there is no reason to allow any party, other than the student, to have direct access (read-only or otherwise) to the student's FSA information. Any legitimate objectives for the OIG recommendation are met by the "MyStudentData Download" functionalities discussed above.

OIG Suggestion

The OIG suggests FSA consider creating preparer-specific access accounts that would allow a student to authorize a preparer to access and modify certain sections of the FAFSA.

FSA Response

FSA does not agree with the OIG's suggestion. We believe such access to an applicant's file/data would compromise the integrity of the Title IV student aid application process. The

student and/or parent maintain complete accountability for the information reported and used to determine eligibility for federal student aid.

In our opinion, it would be contrary to the intent of the Higher Education Act of 1965 (as amended) if FSA provided this type of access to these third parties. It is the applicant that submits the data for the FAFSA. The extensive "smart-logic" of the FAFSA on the Web product maintains the applicant's control of their personal data and FAFSA submissions.

Based on the capability provided through MyStudentData Download, described above, FSA believes that there is sufficient access to the necessary information for counseling and other advisory activities.

Thank you again for the opportunity to share our progress and respond to your recommendations and suggestions.

cc: Dawn Dawson, Audit Liaison Officer
Linda Hall, Internal Review Officer
Fred Anderson, Chief Risk Officer