Review of the Department's Process for Granting Access to the National Student Loan Data System

FINAL INSPECTION REPORT

ED-OIG/I13H0006
July 2008

Our mission is to promote the efficiency, effectiveness, and integrity of the Department's programs and operations.

U.S Department of Education
Office of Inspector General
Washington, DC

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

In accordance with the Freedom of Information Act (5 U.S.C. § 552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Evaluation and Inspection Services

July 24, 2008

Memorandum

TO: Lawrence A. Warder
Acting Chief Operating Officer
Federal Student Aid

FROM: Wanda A. Scott /s/
Assistant Inspector General
Evaluation, Inspection, and Management Services

SUBJECT: Final Inspection Report
Review of the Department's Process for Granting Access to the National Student Loan Data System (Control Number ED-OIG/I13H0006)

Attached is the final inspection report of our Review of the Department's Process for Granting Access to the National Student Loan Data System (NSLDS). We received your comments to our draft report on May 28, 2008. A copy of your response to the draft report in its entirety is attached.

We also received your draft corrective action plan (CAP) with your response. Corrective actions proposed (resolution phase) and implemented (closure phase) will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System (AARTS).

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the reports that remain unresolved after six months from the date of issuance.

In accordance with the Freedom of Information Act (5 U.S.C. §552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation given us during this review. If you or your staff have any questions, please contact W. Christian Vierling, Director, Evaluation and Inspection Services at 202-245-6964.

Enclosure

TABLE OF CONTENTS

EXECUTIVE SUMMARY **1**

BACKGROUND **3**

INSPECTION RESULTS **5**

FINDING 1A – FSA has Weak Controls over the Process of Assigning Lender Identification Numbers **5**

- FSA has not developed adequate procedures to oversee the guaranty agencies' Lender Identification Number applications on behalf of lenders 5
- FSA has not developed effective controls for assigning Lender Identification Numbers 6
- FSA does not verify agreements 6
- Impact of FSA's weak controls over the process of assigning Lender Identification Numbers 7
- Recommendations 7

FINDING 1B – FSA's Process for Granting NSLDS IDs, Passwords, and Access to External Users is Weak **8**

- FSA does not provide adequate oversight of external users 8
- FSA has not established equivalent security requirements for external users to those that are mandatory for internal users 9
- FSA does not require external entities to report on acknowledged internal control weaknesses 12
- Impact of FSA's weaknesses in the process of granting external users access to NSLDS 12
- Recommendations 13

FINDING 2 – FSA Does Not Ensure that External Users Accessing NSLDS Have a Substantially Established Business Relationship with the Borrower **13**

- FSA does not ensure that external users only at lenders and lender servicers with a substantially established business relationship with a borrower have access to the borrower's NSLDS record 13
- Guaranty agencies and state grant agencies have appropriate access to NSLDS 16
- Impact of FSA not ensuring that external users accessing NSLDS have a substantially established business relationship with the borrower 16
- Recommendations 16

DEPARTMENT COMMENTS **18**

OBJECTIVES, SCOPE, AND METHODOLOGY **25**

EXECUTIVE SUMMARY

This report provides the results of our *Review of the Department's Process for Granting Access to the National Student Loan Data System*. Our inspection objectives were to (1) evaluate Federal Student Aid's (FSA) process for granting National Student Loan Data System (NSLDS) IDs and passwords to external users except for schools and borrowers and (2) determine whether the extent of access FSA provides these external users is appropriate.

For our first objective, we found that:

A. FSA has weak control procedures for assigning the Lender Identification Numbers (LIDs) that external entities are required to obtain before applying for access to NSLDS. Specifically, FSA:
   - Has not developed adequate procedures to oversee guaranty agencies' role in the LID assignment process,
   - Has not developed effective controls for assigning LIDs, and
   - Does not verify the required agreements between guaranty agencies and lenders during this process.

B. FSA's process for granting NSLDS IDs, passwords, and access to external users is weak. Specifically, FSA:
   - Does not provide adequate oversight of external users,
   - Has not established equivalent security requirements for external users to those that are mandatory for internal users, and
   - Does not require external entities to report on acknowledged internal control weaknesses.

FSA's weaknesses in granting access to external users increases the risk for inappropriate disclosure or unauthorized use of sensitive and personally identifiable information in NSLDS by external entities.

For our second objective, we found that FSA does not ensure that external users accessing NSLDS have a business relationship with the borrower. Specifically, FSA does not ensure that external users only at lenders and lender servicers with a substantially established business relationship with a borrower have access to the borrower's NSLDS record. Lenders and lender servicers also have access to data that is not required for their Federal Family Education Loan (FFEL) Program business needs. Inappropriate access increases the potential for exposure of sensitive NSLDS data and personally identifiable information, including NSLDS reports that contain the borrower's name, date of birth, and Social Security Number. We found that the access given to guaranty agencies and state grant agencies is appropriate.

We recommend that the Acting Chief Operating Officer for FSA –

1. Develop written procedures for assigning LIDs, including a standard appeal process.

2. Develop procedures to verify and evaluate the adequacy of agreements between the guaranty agency and the lender and between the lender and the beneficial holder in an Eligible Lender Trustee (ELT) arrangement[1] before issuing a Lender Identification Number.

3. Develop and implement control procedures, including edit checks, to monitor access to NSLDS and hold Primary Destination Point Administrators (DPAs)[2] accountable for unauthorized usage.

4. Clarify and strengthen guidance to Primary DPAs to ensure that their users understand and comply with the rules for NSLDS.

5. Develop a requirement for all users to certify that they have read and will comply with the rules and authorized uses of NSLDS and require external users to obtain application and computer security training prior to initial logon.

6. Require external entities to report internal control weaknesses over NSLDS access to FSA. FSA should evaluate the weaknesses and take the appropriate action to safeguard the system.

7. Require lenders, lender servicers, and ELTs to confirm and identify the nature of the substantially established business relationship with the borrower before the borrower's record is accessed.

8. Require lenders to report the date of the signed loan application during the initial request for access to a borrower's record concerning a new or consolidation loan.

9. Require lenders accessing NSLDS concerning new or consolidation loans to maintain the loan applications establishing their business relationship with the borrower.

We provided FSA with a copy of our draft report for comment. FSA did not disagree with our inspection results and concurred with some of our recommendations. FSA stated that there were several recommendations that it could not fully implement because it did not have the regulatory or statutory authority or the recommended solution would have unintended consequences if the changes were implemented as suggested. FSA cited regulatory or statutory issues, but did not provide any examples of unintended consequences that could result from our recommendations. We modified some of our recommendations in response to FSA's comments

[1] An ELT is an arrangement between an eligible FFEL Program lender and an ineligible entity that enables the ineligible entity to participate in the FFEL program. The eligible lender (eligible lender trustee) holds FFEL Program loans in trust for the benefit of the ineligible entity (beneficial holder).

[2] The Primary DPA is the representative at each external entity that is responsible for determining who needs access to NSLDS and the type of access required by each user.

BACKGROUND

Section 485B of the Higher Education Act of 1965 (HEA) authorizes the National Student Loan Data System (NSLDS). NSLDS is a database of information about the Federal financial aid history of Title IV loans and Pell Grants. As the central database for selected Title IV student financial aid, NSLDS stores information about loans, grants, students, borrowers, lenders, guaranty agencies, schools, and servicers. It was designed to provide the following functions: prescreening for Title IV aid eligibility, default rate calculation, operations support, standardized student status confirmation reporting, borrower tracking, pre-claims assistance (PCA) and supplemental PCA, Credit Reform Act support, and preparation of financial aid transcript information.

NSLDS borrower information is organized into sections that include: (1) Loan History, (2) Overpayment History, (3) Pell Grant, and (4) Transfer Student Monitoring. Each section lists the borrower's name, Social Security Number, and date of birth. The web-only view limits users to the Loan History section. The Loan History section reports student status with regard to default, forbearance, and deferment. It is also broken down into aggregate loan information, master promissory note information, and loan summary information.

The aggregate loan information lists the outstanding principal balance and the pending disbursements for subsidized, unsubsidized, Federal Family Education Loan (FFEL) consolidation, combined, and Federal Perkins loans. The master promissory note information describes the notes signed by the borrower. The loan summary information lists the specific loans for the borrower. For each loan, the loan detail information includes type, status, date of origination, school information, disbursed amount, guaranteed amount, outstanding principal balance, the guarantor, and both past and current lenders.

The internal system users of NSLDS include Department of Education (Department), call center, and contractor employees. The external NSLDS users include students, guaranty agencies, schools, third-party servicers, lenders, lender servicers, state grant agencies, and entities in an Eligible Lender Trustee (ELT) arrangement.[3]

Before applying for access to NSLDS, an external entity must first obtain an entity ID number assigned by FSA (*e.g.*, Office of Postsecondary Education ID (OPEID) or Lender Identification Number (LID)). The external entity must then complete the online Student Aid Internet Gateway (SAIG) enrollment application at the Federal Student Aid (FSA) web enroll website. By enrolling the organization in SAIG, the entity can exchange information electronically with the Department. The external entity requests access to NSLDS through this SAIG enrollment process.

[3] An ELT is an arrangement between an eligible FFEL Program lender and an ineligible entity that enables the ineligible entity to participate in the FFEL program. The eligible lender (eligible lender trustee) holds FFEL Program loans in trust for the benefit of the ineligible entity (beneficial holder).

Ongoing Office of Inspector General (OIG) investigations have identified what appear to be unauthorized activities by external NSLDS users. On April 17, 2007, FSA temporarily suspended access to NSLDS by all external entities except schools and borrowers. According to FSA, it needed to examine NSLDS access rules to ensure that the privacy rights of borrowers in NSLDS were being protected, as required by the Privacy Act of 1974, and that users were accessing NSLDS only for authorized purposes.

On May 2, 2007, FSA began to notify entities of the phased-in reinstatement process for access to NSLDS. FSA's policies provided that access to NSLDS would be restored to an entity only after FSA had determined that restoration was appropriate based on its analysis of access and usage information for each entity. FSA started the process with guaranty agencies, followed by lenders and later state grant agencies. As of December 2007, FSA had not developed reinstatement procedures to phase in ELTs and had not determined whether they will be allowed to apply for access to NSLDS.

FSA has been working with guaranty agencies, lenders, and lender servicers to reinstate their access to NSLDS. As of December 26, 2007, 40% of the entity codes that had access to NSLDS on April 17, 2007 had been reinstated.

	Number of entity codes with NSLDS access	
Type of external entity	**April 17, 2007**	**December 26, 2007**
Guaranty Agency	36	36
Lender	239	61
Lender Servicer	24	24
Total	**299**	**121**

FSA revoked access for all state grant agencies on April 17, 2007, and asked the state grant agencies to reapply for NSLDS access. As of December 26, 2007, NSLDS had granted access to eight state grant agencies.

INSPECTION RESULTS

The objectives for this inspection were to (1) evaluate Federal Student Aid's (FSA) process for granting NSLDS IDs and passwords to external users except for schools and borrowers and (2) determine whether the extent of access FSA provides these external users is appropriate. We found that –

1A. FSA has weak control procedures for assigning the LIDs that external entities are required to obtain before applying for NSLDS IDs and passwords that provide access to NSLDS,
1B. FSA's process for granting NSLDS IDs, passwords, and access to external users is weak, and
2. FSA does not ensure that external users accessing NSLDS have a substantially established business relationship with the borrower.

FINDING 1A – FSA has Weak Controls over the Process of Assigning Lender Identification Numbers

In answering our first objective, we found that FSA has weak controls over the process of assigning LIDs. Specifically, FSA –

- Has not developed adequate procedures to oversee the guaranty agencies' LID applications on behalf of lenders
- Has not developed effective controls for assigning LIDs, and
- Does not verify the guaranty agency-lender agreements needed for lender participation in the FFEL Program.

The Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* emphasizes the importance of strong internal controls. The control environment standard states that a "positive control environment is the foundation for all other standards" and "[m]anagement's philosophy and operating style also affect the environment." The "organizational structure" and the "manner in which the agency delegates authority" also affect the control environment. The standards also emphasize the importance of control activities, which "help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results."

FSA has not developed adequate procedures to oversee the guaranty agencies' Lender Identification Number applications on behalf of lenders

To participate as an eligible lender in the FFEL Program, as provided for in 34 C.F.R. § 682.401(b)(19)(A), a lender must work with a guaranty agency to apply for an LID. The regulations at 34 C.F.R. § 682.401(b)(7) state that a lender can participate under reasonable criteria established by a guaranty agency. The regulations specify that the guaranty agency may

evaluate the lender using its own criteria except to the extent that (1) the lender's eligibility has been limited, suspended, or terminated, (2) the lender is disqualified by the Secretary, or (3) the state constitution prohibits the lender's eligibility. The regulations further specify that the guaranty agency may consider the lender's experience in handling loan programs and the percentage of loans currently in delinquent or default status. FSA, however, does not know what criteria the guaranty agencies are using to evaluate lenders in this area because FSA has not developed procedures to assess the criteria being used by guaranty agencies in evaluating lenders.

FSA has not developed effective controls for assigning Lender Identification Numbers

FSA's Office of the Chief Financial Officer (OCFO) requires guaranty agencies to submit LID applications on behalf of lenders. FSA has delegated the responsibility of assigning LIDs to one primary staff member in FSA's OCFO without developing formal written policies and procedures for assigning LIDs. Although FSA has an informal appeal process for lenders who are denied an LID, FSA has not established a standard appeal process.

Weak control activities over the assignment of LIDs are a threat to controlling access to NSLDS because obtaining an LID is required for lenders to participate in the FFEL Program and gain access to NSLDS. Without written procedures, FSA has no assurance that the process of assigning LIDs is performed systematically to ensure that only eligible entities are allowed to apply for NSLDS access. Assigning responsibility to a single person without documented procedures makes FSA vulnerable if the individual is not available to perform these functions. Without segregation of duties, assignment of LIDs is susceptible to error and abuse. Weak control procedures increase the chance that risks may not be systematically identified and may jeopardize the sensitive data and personally identifiable information contained within NSLDS.

FSA does not verify agreements

The regulations at 34 C.F.R. § 682.401(b)(19) state that a guaranty agency must ensure "that all lenders in its program meet the definition of 'eligible lender' in section 435(d) of the [HEA] and have a written lender agreement with the agency." To become an eligible lender, a lender must sign an agreement with a guaranty agency as part of the LID application process. FSA neither verifies that the lender and guaranty agency have signed an agreement nor requests or receives a copy of the agreement. As a result, FSA does not know whether the guaranty agency and lender have an ongoing agreement, what is in the agreement, and for what the guaranty agencies are holding lenders accountable. While the regulations do not state what must be in the agreements, FSA has no assurance that the agreements are in line with the requirements of the FFEL Program, that lenders understand their responsibilities for compliance under the program, or whether the agreements are consistent across guaranty agencies and lenders.

When issuing LIDs for ELT arrangements, FSA does not verify or request a copy of the ELT agreement. FSA does not have a formal relationship with beneficial holders. As specified in 34 C.F.R. § 682.203(b), a lender that holds a loan in its capacity as a trustee assumes responsibility for complying with all statutory and regulatory requirements imposed on any other holders of a loan. Because FSA does not verify or request a copy of the ELT agreements, FSA does not know what is in the agreements and has no assurance that the lender trustees have informed the beneficial holders of FFEL Program requirements or included provisions to ensure compliance

by the beneficial holders. FSA cannot evaluate whether the agreements between lender trustees and beneficial holders would require that the ELT receive an LID or whether the lender trustee will monitor the actions of the beneficial holder to ensure FFEL Program integrity.

FSA's General Manager of Business Operations informed us that NSLDS staff allowed beneficial holders to gain access to NSLDS because she understood that FSA's OCFO verified the ELT agreements and had determined that the ELT was an eligible FFEL Program participant because it was issued an LID. As a result, Business Operations and NSLDS staff members incorrectly assume ELT agreements are verified during the LID issuance process.

FSA's control environment is weak due to management's operating style of not requiring lenders to submit required agreements with guaranty agencies and other documentation to verify conditions of eligibility and assuming without verification that organizational components have made critical eligibility determinations. The delegation of responsibility for assigning LIDs to one primary staff member without formal written policies and procedures also indicates a weak control environment. In addition, the lack of segregation of duties and responsibilities is a control activity weakness that increases the risk of error and abuse.

Impact of FSA's weak controls over the process of assigning Lender Identification Numbers

FSA's weak control environment contributes to the inadequate control activities and the lack of policies and procedures used to control the process of assigning LIDs. The weak controls impact and affect all Department systems accessible by lenders. The weak controls could permit unauthorized access or pass vulnerabilities to the NSLDS system, which stores borrower loan information and information protected by the Privacy Act of 1974.

Recommendations

We recommend that the Acting Chief Operating Officer for FSA –

1.1 Develop written procedures for assigning LIDs, including a standard appeal process.

1.2 Develop procedures to verify and evaluate the adequacy of agreements between the guaranty agency and the lender before issuing an LID.

1.3 Develop procedures to verify and evaluate the adequacy of ELT agreements between the lender and the beneficial holder before issuing an LID.

1.4 Obtain and verify current agreements between guaranty agencies and lenders and between lenders and beneficial holders in an ELT arrangement.

FINDING 1B – FSA's Process for Granting NSLDS IDs, Passwords, and Access to External Users is Weak

In reviewing FSA's process for granting NSLDS IDs and passwords to external users, we found that FSA –

- Does not provide adequate oversight of external users,
- Has not established equivalent security requirements for external users to those that are mandatory for internal users, and
- Does not require external entities to report on acknowledged internal control weaknesses.

FSA does not provide adequate oversight of external users

FSA employs a model where a representative from each external entity, known as the Primary Destination Point Administrator (DPA), is responsible for determining who needs access to NSLDS and the type of access required by each user. FSA requires the Primary DPAs to enroll users at their entities and relies on the Primary DPAs to know which entity employees need access to NSLDS. FSA expects the Primary DPAs to evaluate and verify prospective users' need for access and then to submit the users' information and application to FSA on the users' behalf. FSA receives applications from the Primary DPAs for review and approval. Once an external user is approved for NSLDS access, NSLDS generates the User ID and the staff mails the User ID directly to the external user. In a separate mailing, the NSLDS staff provides an initial password to the external user, along with the "Instructions for NSLDS Users," which describes the rules and authorized uses of NSLDS. FSA does not require external users to sign a statement certifying that they have read and will comply with the instructions.

FSA trusts the Primary DPAs to oversee user NSLDS access at their entities, but has not provided guidance on what the Primary DPA's specific oversight activities should entail. The only assurance FSA has that Primary DPAs will fulfill their responsibilities and ensure that the users adhere to the rules and authorized use of NSLDS is a certification provided with the application from the entity's Chief Executive Officer (CEO) and Primary DPA.

Prior to the shutdown of NSLDS on April 17, 2007, Primary DPAs were required to sign a statement certifying that they agreed to the Primary DPA responsibilities and would comply with applicable rules and regulations. This certification applied to systems in FSA's Electronic Data Exchange (EDE), such as NSLDS. FSA did not require Primary DPAs to sign a certification specifically for NSLDS. These were the only instructions provided to Primary DPAs regarding their roles and responsibilities.

Due to concerns about access to NSLDS and potential misuse of the system, FSA issued *Dear Colleague Letter GEN-05-06/FP-05-04* in April 2005 to remind the financial aid community that NSLDS users are responsible for using their access properly and for protecting the sensitive data and personally identifiable information contained in the system. FSA, however, has no assurance that all NSLDS users received actual notice of the letter since the letter was only posted to a website or sent to individuals on a listserv.

The materials provided to external entities for reinstatement to NSLDS have provided strong and clear requirements to the entity leaders and Primary DPAs. The reinstatement materials clearly describe the authorized uses of NSLDS, user responsibilities, and the penalties associated with misuse of NSLDS. Although the reinstatement materials are a good start, FSA has infrequent communication with Primary DPAs and does not provide guidance to DPAs on the specific actions FSA would expect DPAs to perform in monitoring their users. The reinstatement materials also do not provide any provision for external users to certify that they know and understand their NSLDS responsibilities.

FSA has proposed, but not yet implemented, an active Primary DPA recertification process where Primary DPAs will be required to annually recertify that each of their users still requires NSLDS access or FSA will terminate the user's access. Prior to the temporary suspension of access to NSLDS, FSA utilized a passive user recertification process. Under this process, the Primary DPA annually received a listing of the entity's users, but the Primary DPA was not required to validate that the organization's users still needed access and the information was accurate.

FSA has partnered with external entities and Primary DPAs to more easily manage the user enrollment process, but FSA has not implemented the proper controls to manage the high risks associated with trusting and providing this level of control to Primary DPAs. Without proper oversight, the Primary DPA model introduces an opportunity for entities and users to abuse their access to NSLDS. The steps that FSA has taken to reinstate access to the entities do not provide adequate oversight of Primary DPAs because FSA has not developed any control activities to ensure that Primary DPAs are fulfilling their NSLDS responsibilities.

FSA has not established equivalent security requirements for external users to those that are mandatory for internal users

The security requirements for external users are much weaker than the requirements for internal users with the same level of NSLDS access. FSA checks to ensure that external users do not have a defaulted student loan, but FSA does not require external users to:

- Certify that they have read and will comply with the rules and instructions for NSLDS,
- Obtain favorable background checks, and
- Take any application or computer security training.

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, emphasizes the importance of strong security controls and describes the minimum controls for Federal government information systems. Office of Management and Budget (OMB) Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources* also "establishes a minimum set of controls to be included in Federal automated information security programs" and requires agencies to "implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications."

Internal user view-only web access is similar to the external user view-only web access, except that different reports are available to internal users based on the user's organizational classification. All internal users complete a User Participation Request Form that lists their current Department clearance level, along with their name, title, work information, Social Security Number, mother's maiden name, date of birth, organization, and supervisor's signature. The internal user applicant is required to read and sign Appendix A: Rules of Behavior to complete the NSLDS application package. Before granting access to NSLDS and creating a user password, the NSLDS System Security Officer reviews the forms and confirms the internal user's security clearance and date of clearance with Human Resources Personnel Security.

FSA does not require external users to certify that they have read and will comply with the rules and instructions for NSLDS

NIST describes the planning requirements for rules of behavior:

> The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Although all NSLDS users electronically certify at login that they are accessing a restricted system and are consenting to the Privacy Act's requirements, external users are not required to certify that they have read and complied with system rules and responsibilities.

Section 2.3 of the NSLDS Security Plan requires that all internal users sign the NSLDS Rules of Behavior Form during the NSLDS ID application process, but it does not include a similar requirement for external users. As part of the application process, all external users are required to sign a document certifying that they have read the rules and responsibilities for FSA EDE systems. This certification is then maintained by the Primary DPA. Although NSLDS external users certify that they have read and will adhere to the Privacy Act's requirements, NSLDS external users are not required to sign a document or electronically certify that they have read and will comply with the authorized uses of NSLDS.

FSA does not comply with the NIST standard because it does not require external users to certify that they have read and will comply with the rules and authorized uses of NSLDS before accessing the system. Therefore, FSA cannot ensure that external users understand their roles and will responsibly use the system for only authorized purposes. If external users were required to sign a certification for proper NSLDS usage like internal users, it would help hold individuals accountable for their actions and help ensure that each user was completely aware of his or her responsibilities.

FSA does not require external users to obtain favorable background checks

NIST provides the following requirements for personnel security: "The organization screens individuals requiring access to organizational information and information systems before authorizing access." Departmental Directive OM:5-101, *Contractor Employee Personnel*

Security Screenings, specifies that contractor employees that require access to Privacy Act-protected information obtain at least a 5C security clearance for Moderate Risk positions. Although external users of NSLDS also have access to Privacy Act information, external users are not subject to any additional security checks before gaining access to NSLDS.

FSA does not require external users to take any application or computer security training
NIST provides the following requirements for security awareness and training: "The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [at least annually] thereafter." In addition, OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources* requires specialized training requirements to be included in system security plans:

> Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).

External users, unlike internal users, are not required to complete application or computer security training prior to accessing NSLDS. Though the NSLDS Security Plan has several sections devoted to security and application training, it requires mandatory, annual computer security awareness training only for internal users (Department and contractor employees). Section 3.8.2 of the NSLDS Security Plan specifies that contractor employees will receive annual security training for the following topics: NSLDS Security Training, General Security, Personnel Security, User IDs and passwords, System Security (application protection levels and functional groups), Physical Security, and the Privacy Act Statement – Non-Disclosure Statement.

Section 4.1.2.4 of the NSLDS security plan provides the following for external user training: "Users of NSLDS Financial Aid Professional Web site receive instruction via the Help pages." External users are not required to receive training to access the system, but instead receive instruction only through help pages. The help pages include a link that directs the user to a general Department page on site security and intrusion detection. The Department's page does not include specific security information for NSLDS. Though Section 3.8.1 of the NSLDS Security Plan explains that NSLDS staff will deliver a comprehensive awareness program at conferences, such as with the National Association of Student Financial Aid Administrators (NAFSAA) conferences, FSA cannot ensure that all external users receive training on both NSLDS application features and system security.

FSA does not comply with the security training requirement for external users, as specified in the NIST standard. FSA does not require external users to take NSLDS application and computer security training at least once before gaining access to the system as it does for internal users. Therefore, FSA has no assurance that external users are aware of the security requirements or

will comply with computer security rules and will safeguard the sensitive data and personally identifiable information contained in NSLDS.

FSA does not require external entities to report on acknowledged internal control weaknesses

The independent auditors for entities are required to report material internal control weaknesses in the financial statement audit, but only as they relate to the financial statements. The NSLDS Access Certification requires the Primary DPA and the CEO to certify:

> We have disclosed to our independent auditors and to any audit committee all significant deficiencies in the design and operation of the internal controls that could adversely affect the ability of the agency to ensure compliance with the requirements for NSLDS access, as well as any fraud, whether or not material, that involves management or any other employee connected to the agency's access to NSLDS.

The Director of NSLDS stated that she expects independent auditors to properly disclose any deficiencies to FSA through the financial statement audit. She stated that she also expects that the FSA Office of Program Compliance will take the necessary steps to evaluate the entity's internal control weaknesses. The Director of NSLDS explained that FSA does not require external entities to directly report internal control weaknesses to FSA, but that the internal control weaknesses would be reported in the financial statement audit. The Department does not receive financial statement audits from lenders, lender servicers, ELTs, or beneficial holders. The Department does receive compliance audits from lenders and lender servicers. In addition, the guide for these compliance audits does not require any internal control reporting.

The internal control weaknesses that would be reported to FSA as part of a financial statement audit conducted in compliance with Generally Accepted Government Auditing Standards would be only those weaknesses that would have a material effect on the financial statements taken as a whole. There could be weaknesses in the internal controls at an external entity that are not material to the financial statements, but could be a significant NSLDS security concern to the Department.

Impact of FSA's weaknesses in the process of granting external users access to NSLDS

The weaknesses in the process are caused by FSA's lack of oversight of external entities, such as lenders, lender servicers, and beneficial holders. FSA's enrollment model lacks checks or controls to ensure that external users know their roles and responsibilities. In addition, FSA does not sufficiently oversee the Primary DPAs as discussed in Finding 1A. There is a risk that the process can be misused by external entities to use sensitive and personally identifiable information in NSLDS for unauthorized purposes. OIG is currently conducting criminal investigations into allegations of unlawful access and use of NSLDS. During the course of these open investigations, OIG has identified DPAs that have criminal records for various felony offenses. These offenses include burglary, passing worthless checks, and sale/distribution and possession of cocaine.

In addition, FSA has not yet implemented several enhancements and controls within NSLDS. FSA officials have also said that new systems, Integrated Partner Management (IPM) and Security Architecture, which have not yet been developed, will create a stronger control environment for NSLDS. Overall, FSA has not implemented all of the necessary controls required for the security of the system.

Recommendations
We recommend that the Acting Chief Operating Officer for FSA –

1.5 Clarify and strengthen guidance to Primary DPAs to ensure that their users understand and comply with the rules for NSLDS.

1.6 Develop and implement control procedures, including edit checks, to monitor access to NSLDS and hold Primary DPAs accountable for unauthorized usage.

1.7 Develop a requirement for all users to certify that they have read and will comply with the rules and authorized uses of NSLDS and require external users to obtain application and computer security training prior to initial logon.

1.8 Require external entities to report all internal control weaknesses over NSLDS access to FSA. FSA should evaluate the weaknesses and take the appropriate action to safeguard the system.

FINDING 2 – FSA Does Not Ensure that External Users Accessing NSLDS Have a Substantially Established Business Relationship with the Borrower

Our second objective was to determine whether the extent of access FSA provides these external users is appropriate. We determined that FSA does not ensure that external users only at entities with a substantially established business relationship with a borrower have access to the borrower's NSLDS record. Lenders and lender servicers also have access to data that is not required for their FFEL Program business needs.

The GAO *Standards for Internal Control in the Federal Government* specify that there should be "restrictions on users to allow access only to system functions that they need." In addition, "[a]ccess to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained."

FSA does not ensure that external users only at lenders and lender servicers with a substantially established business relationship with a borrower have access to the borrower's NSLDS record
The NSLDS data available to lenders and lender servicers includes enrollment status, loan repayment status, and the borrower's FFEL Program loan history including loans not held by the lender or serviced by the lender servicer. Lenders and lender servicers are limited to view-only access in NSLDS and do not have updating capabilities like schools and guaranty agencies.

Before suspension of access, users at beneficial holders in an ELT arrangement also had the same NSLDS access as lender and lender servicers.

There are three primary business relationships that lenders and lender servicers have with borrowers: (1) originating and disbursing loans, (2) servicing loans, and (3) consolidating loans. The NSLDS reinstatement materials further break down these duties and specify that access for users at lender and lender servicers is limited to the following six activities: (1) consolidating lender, (2) loan holder, (3) enrollment, (4) accuracy, (5) deferments, and (6) default rates.

Originating and disbursing loans. Lenders are responsible for originating and disbursing loans. In relation to these duties, part of a lender's due diligence includes checking student eligibility and ensuring that there is a valid signed promissory note. To be eligible for a FFEL Program loan a borrower must not exceed the aggregate and annual loan amounts, must be enrolled at an eligible institution, and must not be in default on any Title IV loans. Lenders may use NSLDS for evaluating borrower eligibility, although the Department's policy is that lenders can rely on a school's certification of a borrower's eligibility because schools are required to make this determination before certifying a loan application.

An originating and disbursing lender in the FFEL Program would require only four pieces of information from NSLDS: (1) aggregate loan amounts, (2) annual loan amounts, (3) enrollment status, and (4) default status. As noted above, lenders currently have access to additional information in a borrower's record that is not needed to establish borrower eligibility.

Servicing loans. To service a loan, a lender needs information on a borrower's enrollment status, default status, and whether the borrower has been granted deferment or forbearance. In addition, much of the current lender use of NSLDS is in relation to a lender's customer service and counseling functions, which require access to information in the borrower's NSLDS record. To perform servicing functions, lenders do not need access to information on loans they do not hold. Therefore, lender access to NSLDS should be limited to only the loans they hold and summary data of the borrower's loan history.

Lender customer service and counseling would be limited to the loans a lender holds unless a lender is counseling a borrower regarding consolidation. Since the lenders have the most current loan detail information on the loans they hold, they do not need loan detail information from NSLDS to counsel borrowers. Should a lender determine that access to the borrower's entire loan history would assist in counseling a borrower, the lender should first receive permission from the borrower. The borrower should directly notify NSLDS to provide the lender with access to the borrower's entire loan history.

Consolidating loans. A consolidating lender requires access to a borrower's full loan history, including loans not held by the lender. Presently, a consolidating lender needs a borrower's signed and completed application in order to access the borrower's record for consolidation purposes.

FSA does not ensure that a borrower's NSLDS record is accessed only by lenders and lender servicers with one of the above business relationships with the borrower. According to FSA's Ombudsman, borrowers have unwittingly allowed a consolidating lender to access their records without a full understanding of the process. The Ombudsman explained that in some cases marketers purchase partial information from credit bureaus and call borrowers on the phone, talk very rapidly, and portray themselves as being associated with the Department. An Ombudsman Specialist stated that the marketer will lead students into thinking that they will receive more information about a consolidation loan. Though marketing is an explicitly prohibited activity, marketers have used this method to obtain the information necessary to access a borrower's record in NSDLS.

FSA has informed consolidating lenders that they should access NSLDS only when they have received a signed consolidation application. Apart from the instructions to the lenders, FSA does not have controls to prevent or monitor whether consolidating lenders access borrower records prior to receipt of the signed application and has no assurance that the student is aware that the lender has access to his or her record in NSLDS. To ensure the security of the system and the borrower, the signed application should be dated and steps taken to ensure access is appropriate and does not occur before the application date. Such action could entail requiring the lender to enter the consolidation application date before being granted access to the borrower's entire loan history in NSLDS, or having the borrower notify FSA to grant permission for the lender to access the borrower's entire loan history. FSA could also confirm the borrower's authorization in writing to verify the action with the borrower. In addition, a borrower's record should be limited to one consolidating lender at any time and access to the lender can be provided on a time-limited basis.

Beneficial holders in an Eligible Lender Trustee agreement

Prior to the April 2007 shutdown of NSLDS, beneficial holders had the same level of access as lenders. According to data provided by FSA, 237 of 5,574 users at entities in an ELT agreement were classified as potential abusers. Of the 1,752 users at lenders not in an ELT agreement, FSA identified only 14 potential abusers.

Beneficial holders do not have a formal relationship with the Department but are participants in the FFEL Program by virtue of the ELT agreement with an eligible lender. FSA does not obtain or verify the ELT agreement to ensure that the beneficial holder has legitimate FFEL Program functions that would require access to NSLDS. FSA has no assurance that beneficial holders in an ELT relationship have a legitimate, substantially established business relationship with a borrower and therefore should have access to the borrower's record.

In order for a non-consolidating lender to perform its duties, it needs access only to the loans it holds and summary default information on aggregate loan amounts, annual loan amounts, enrollment status, and whether the borrower is in default, forbearance, or deferment. Providing access to borrower data to lenders, lender servicers, and ELTs without controls to confirm a viable business relationship with the borrower is a weakness in FSA's internal controls.

Guaranty agencies and state grant agencies have appropriate access to NSLDS
Guaranty agencies have access to a borrower's full loan history and have the ability to update a borrower's NSLDS record. According to the regulations, guaranty agencies are responsible for guaranteeing a loan and for reviewing school and lender eligibility. In the NSLDS reinstatement materials, the specific user functions for guaranty agencies are limited to the following activities:

1. Determining a person's eligibility for Title IV student aid
2. Billing and collecting on a Title IV loan or grant
3. Enforcing the terms on a Title IV loan
4. Submitting student enrollment information
5. Ensuring the accuracy of a financial aid or borrower record
6. Assisting with default aversion activities
7. Obtaining default rate information
8. Updating an NSLDS record
9. Teacher Loan Forgiveness Update
10. Compliance

In order to accomplish their duties, including updating borrower records and compliance, guaranty agencies require access to a borrower's NSLDS record. As of September 6, 2007, all 35 guaranty agencies have been re-enrolled into the system.[4]

According to the NSLDS reinstatement materials, state grant agencies functions are limited to (1) default/overpayment status of loans, (2) enrollment, (3) loan forgiveness or loan cancellation, and (4) other activities consistent with the guidance provided in the materials. Access by state grant agencies is limited to records of in-state residents, non-residents who list an institution that is within the state but do not indicate that state as their legal residence, and students who sign a form releasing their data. As of December 26, 2007, eight state grant agencies had re-enrolled into the system.

Impact of FSA not ensuring that external users accessing NSLDS have a substantially established business relationship with the borrower
Access by entities without a substantially established business relationship with a borrower opens NSLDS up to increased exposure of sensitive data and personally identifiable information. Lenders and lender servicers, in terms of volume and self-interest, are the most risky of the external entities.

Recommendations
We recommend that the Acting Chief Operating Officer for FSA –

2.1 Require lenders, lender servicers, and ELTs to confirm and identify the nature of the substantially established business relationship with the borrower before the borrower's record is accessed.

[4] One guaranty agency has two Guarantor Identification Numbers.

2.2 Require lenders to report the date of the signed loan application during the initial request for access to a borrower's record concerning a new or consolidation loan.

2.3 Require lenders accessing NSLDS concerning new or consolidating lenders to maintain the loan applications establishing their business relationship with the borrower.

DEPARTMENT COMMENTS

On April 14, 2008, we provided FSA with a copy of our draft report for comment. FSA provided its comments to the report on May 28, 2008. FSA did not disagree with our inspection results and concurred with some of our recommendations. A copy of FSA's comments, in their entirety, is attached to this report.

General Comments

FSA stated that there were several recommendations that it could not fully implement because it did not have the regulatory or statutory authority or the recommended solution would have unintended consequences if the changes were implemented as suggested. FSA cited regulatory or statutory issues for recommendations 1.2, 1.3, and 1.4, but did not provide any examples of unintended consequences that could result from our recommendations.

Recommendation 1.1

Develop written procedures for assigning LIDs, including a standard appeal process.

FSA Comments

FSA agreed with this recommendation. FSA stated that in January 2008, it developed and implemented written procedures for assigning LIDs, including a challenge/appeal process.

OIG Response

While FSA has developed written procedures for assigning LIDs, the procedures do not address Recommendations 1.2 and 1.3. FSA's procedures should require the lender, guarantor, or the beneficial holder in an ELT arrangement to submit agreements between the guaranty agency and the lender and between the lender and the beneficial holder. For example, FSA does not know the criteria for which lenders are holding beneficial holders accountable, and there is no mention in the policies and procedures about informing lenders throughout the process that they are responsible for the compliance of any beneficial holders participating through them. FSA also does not know the criteria for which guaranty agencies are holding lenders accountable. No changes have been made to the recommendation.

Recommendation 1.2

Develop procedures to verify and evaluate the adequacy of agreements between the guaranty agency and the lender before issuing an LID.

FSA Comments

FSA did not agree with this recommendation as written. FSA stated that under the regulations at 34 CFR § 682.401(b)(19),[5] a guaranty agency is required to have a written agreement with each lender that participates in the loan program through that guaranty agency, and the Department has the authority to review those agreements to ensure they exist. FSA stated that the

[5] There is a typographical error in both of FSA's references to this regulation in its comments.

regulations, however, do not have specific standards for those agreements, and therefore, FSA has limited authority to regulate the adequacy of the agreements between the guaranty agency and lender beyond the existing statutory and regulatory requirements.

OIG Response

No changes have been made to this recommendation. We recognize that FSA has limited regulatory authority over the agreements between guaranty agencies and lenders. To clarify, OIG did not recommend regulatory changes. FSA does, however, have the authority to review agreements to ensure that, at the least, guaranty agencies inform lenders of their responsibility to be in compliance with the requirements of the HEA, regulations, and subregulatory guidance such as the NSLDS rules.

The HEA, regulations, and subregulatory guidance provide ample criteria for FSA to evaluate whether the agreements between guaranty agencies and lenders are adequate to protect the federal interest.

For example, the regulations at 34 C.F.R. § 682.414(a)(4) specify that a guaranty agency require a participating lender to maintain current, complete, and accurate records of each loan that it holds. The regulations at 34 C.F.R. § 682.414(c)(2) specify that a guaranty agency require in its agreement with a lender, or in its published rules or procedures, that the lender or its agent give the Secretary or the Secretary's designee and the guaranty agency access to the lender's records for inspection and copying in order to verify the accuracy of the information provided by the lender pursuant to Sec. 682.401(b) (21) and (22), and the right of the lender to receive or retain payments made under this part, or to permit the Secretary or the agency to enforce any right acquired by the Secretary or the agency under this part. A review would ensure that the guaranty agency has included provisions to comply with these requirements. A review also provides FSA with an opportunity to ensure that agreements do not contain inducements prohibited by § 428(b)(3) of the HEA and 34 C.F.R. §682.401(e).

Recommendation 1.3

Develop procedures to verify and evaluate the adequacy of ELT agreements between the lender and the beneficial holder before issuing an LID.

FSA Comments

FSA did not fully concur with this recommendation. FSA stated that it has developed and implemented revised procedures for reviewing ELT agreements between the lender and the beneficial holder before issuing an LID. FSA stated that the revised procedures now require that FSA receive copies of the agreements, financial statements, financing plans, and co-signed documents acknowledging the working partnership between the entities. FSA added that with respect to the evaluation of the adequacy of the ELT agreements, the regulations do not have specific standards for those agreements, and therefore, FSA has limited authority to regulate the adequacy of the agreements between the lender and the beneficial holder.

OIG Response

No changes have been made to this recommendation. We recognize that FSA has limited regulatory authority over the agreements between lenders and beneficial holders in an ELT

arrangement. OIG did not recommend regulatory changes. As noted above, however, FSA has the authority to review agreements to ensure that lenders have informed beneficial holders that they must be in compliance with any requirements of the HEA, regulations, and subregulatory guidance such as NSLDS rules. A review also provides FSA with an opportunity to ensure that agreements do not include inducements prohibited by § 435(d)(5) of the HEA and 34 C.F.R. § 682.200.

The policies and procedures cited by FSA do not require the lender, guarantor, or the beneficial holder in an ELT arrangement to submit the agreement between the lender and the beneficial holder. FSA does not know the criteria for which lenders are holding beneficial holders accountable, although the regulations at 34 C.F.R. 682.203(b) specify that the lender in its capacity as trustee assumes responsibility for compliance with all statutory and regulatory requirements. FSA's Lender Assignment Procedures state, "In all cases it should be stressed to the lender that they bear a significant responsibility to 'know their client.'" There is no mention in the procedures about informing lenders throughout the process that they are responsible for the compliance of any beneficial holders participating through them.

Recommendation 1.4

Obtain and verify current agreements between guaranty agencies and lenders and between lenders and beneficial holders in an ELT arrangement.

FSA Comments

FSA did not concur with OIG's recommendation as written. FSA stated that under the regulations at 34 C.F.R. § 682.401(b)(19),[6] a guaranty agency is required to have a written agreement with each lender that participates in the loan program through that guarantee agency, and the Department has the authority to review those agreements to ensure they exist. FSA stated that the regulations, however, do not have specific standards for those agreements, and therefore, FSA has limited authority to regulate the adequacy of the agreements between the guaranty agency and lender beyond the existing statutory and regulatory requirements.

OIG Response

No changes have been made to this recommendation. While recommendations 1.2 and 1.3 are forward looking and would require a process for new LID applicants, this recommendation addresses the lack of information FSA has on the agreements between guaranty agencies and lenders and between lenders and beneficial holders in an ELT agreement. As noted above, we recognize that FSA has limited regulatory authority over the agreements between guaranty agencies and lenders and between lenders and beneficial holders in an ELT arrangement. Again, FSA has the authority to review agreements to ensure that guaranty agencies require compliance with the HEA, regulations, and subregulatory guidance from lenders currently participating in the FFEL program. FSA should do no less for the agreements between lenders and beneficial holders currently in an ELT arrangement.

[6] There is a typographical error in both of FSA's references to this regulation in its comments.

Recommendation 1.5
Clarify and strengthen guidance to Primary DPAs to ensure that their users understand and comply with the rules for NSLDS.

FSA Comments
FSA did not disagree with this recommendation. FSA stated that in January 2008, procedures for enrolling users for access to FSA systems through the SAIG enrollment process were clarified and strengthened. FSA stated that NSLDS, among other systems, utilizes this method to provide access to external partners. FSA also stated that DPA responsibilities and additional requirements for the Primary DPA and CEO were strengthened and clarified. FSA stated that the signature process was improved to ensure the CEO or proper designee is accountable for the users' access. FSA also stated that the FSA user statement clarified information regarding the appropriate uses of FSA systems and the protection of Privacy Act information.

OIG Response
We agree that the instructions to DPAs and users are stronger. We still recommend that FSA provide additional guidance to DPAs, *e.g.*, providing the DPA with examples of non-compliant actions and methods to identify potential problem users. No changes have been made to the recommendation.

Recommendation 1.6
Develop and implement control procedures, including edit checks, to monitor access to NSLDS and hold Primary DPAs accountable for unauthorized usage.

FSA Comments
FSA agreed to implement control procedures to monitor access to NSLDS. FSA disagreed with the recommendation for holding the Primary DPAs accountable for unauthorized usage. FSA stated that it holds the CEO or designee accountable for the user's access, and, in accordance with *Dear Colleague Letter GEN-05-06/FP-05-04*, holds the organization as well as individual users responsible.

FSA stated that reports will be made available for Primary DPAs to monitor the usage and potential access violations, and expected to have this completed by December 31, 2008. FSA added that when the reports are available, it will send the Primary DPAs an email to let them know that the reports are available and inform them that FSA expects them to use the reports to monitor usage and potential access violations.

OIG Response
We agree that the CEO or designee should be held accountable for the NSLDS users' access; however, the CEO or designee should not be the sole person responsible. Given the critical role assigned to the Primary DPA as the frontline administrator of a lender or guaranty agency's access to NSLDS, the Primary DPA should also be held accountable for unauthorized usage. The Primary DPA is responsible for determining who needs access to NSLDS and the type of access required by each user. The Primary DPA enrolls users and verifies their duties. And, as stated in FSA's response, FSA expects the Primary DPA to monitor usage and potential access violations. No changes have been made to the recommendation.

Recommendation 1.7
Develop a requirement for all users to certify that they have read and will comply with the rules and authorized uses of NSLDS and require external users to obtain application and computer security training prior to initial logon.

FSA Comments
FSA agreed with this recommendation. FSA stated that by December 2008, NSLDS will develop a certification page with the rules and authorized uses of NSLDS that users will have to accept at logon to begin to access the NSLDS website. FSA stated that this certification page will also provide a computer security training download component: The user will certify that they read, understood and agreed to the application and security training.

OIG Response
No changes have been made to this recommendation.

Recommendation 1.8
Strengthen the requirements of the Primary DPAs to ensure that policies and procedures are in place to assure that new users understand the sensitive nature of NSLDS and the penalties for misuse of the system.

FSA Comments
FSA agreed with this recommendation. FSA stated that in January 2008, it implemented new procedures that require the Primary DPA to be responsible for obtaining and storing a signed User Responsibility Statement for each user that registers for access to FSA systems via the SAIG enrollment process. FSA added that NSLDS now directs all new NSLDS User IDs to the Primary DPA who is responsible for delivery of the User ID and the NSLDS Rules of Behavior to each new user.

OIG Response
FSA's comments satisfied the intent of our recommendation, although we have not evaluated the effectiveness of FSA's procedures. We have removed this recommendation and renumbered Recommendation 1.9.

Recommendation 1.9
Require external entities to report all internal control weaknesses over NSLDS access to FSA. FSA should evaluate the weaknesses and take the appropriate action to safeguard the system.

FSA Comments
FSA agreed with this recommendation. FSA stated it will provide language to OIG to include this step in the A-133 Lender/Servicer Audit Guides.

OIG Response
No changes have been made to this recommendation. In developing its corrective action, we suggest that FSA ensure that requirements for all entity compliance audits are included; these entities include lenders, lender servicers, guaranty agencies, and guaranty agency servicers.

Recommendation 2.1
Develop and implement a process to confirm that lenders, lender servicers, and ELTs have an ongoing business relationship with the borrower before the borrower's record is accessed.

FSA Comments
FSA disagreed with this recommendation. FSA stated that the relationship with the borrower begins with the loan application and/or guaranty process. FSA added that lenders and servicers need to view data on NSLDS to determine eligibility of a loan or provide proper servicing of FFEL loans to a borrower.

FSA proposed developing a monitoring tool to identify instances of borrower access where no relationship exists or was recently established after records were accessed. FSA stated it will then contact the institution to request additional information and to determine appropriate next steps. FSA anticipates having this tool in place by December 2008.

OIG Response
We agree that a lender's relationship with the borrower begins with the loan application process. We have changed the terminology in the report to refer to external entities having a "substantially established business relationship" with the borrower. FSA should ensure that lenders, lender servicers, and ELTs have a substantially established business relationship with the borrower before the borrower's record is accessed. FSA should require lenders, lender servicers, and ELTs to confirm that they have a substantially established business relationship with the borrower before the borrower's record is accessed. FSA should require entities to confirm that they are either making a new loan, servicing an existing loan, or consolidating a borrower's loans. For both consolidating and non-consolidating lenders, FSA should require the lender to report the application date when they established the business relationship with the borrower. We have modified our original recommendation.

Recommendation 2.2
Modify NSLDS to allow only the loan holding lender and its servicer to view the borrower's summary default view and only those loans that the borrower holds with the individual lender.

FSA Comments
FSA disagreed with this recommendation. FSA stated that lenders and servicers rely on data in NSLDS to grant deferments and forbearances, consolidate loans, and provide customer service to borrowers and schools. FSA stated that by providing only limited information, the lender will not see loan statuses of deferment or forbearance on loans they do not hold. FSA added that they will also not be able to determine the validity of Loan Verification Certificates or consolidation loan applications. FSA recommended that NSLDS create a monitoring tool to identify instances of borrower access where no relationship exists or was recently established after records were accessed.

OIG Response
As a result of our revised Recommendation 2.1, we have removed this recommendation and renumbered the Finding 2 recommendations.

Recommendation 2.3
Provide a borrower or prospective borrower the ability to authorize NSLDS to provide one lender access to his or her records for consolidation and counseling purposes for a limited amount of time.

FSA Comments
FSA disagreed with this recommendation. FSA stated that it is acceptable for a lender to access a record on NSLDS once it has received a substantially complete, signed consolidation loan application, and that the loan application signed by the borrower gives the lender permission to access his/her records. FSA stated that requiring the borrower to authorize access to NSLDS for one lender to view NSLDS negates the permission already provided by the loan application and places an additional burden on the borrower.

OIG Response
The purpose of our recommendation was to ensure that borrowers had granted permission to consolidating lenders before allowing access to their NSLDS record. We recognize that a substantially complete, signed application can provide this permission. As such, FSA should require both consolidating and non-consolidating lenders to maintain signed applications that document the business relationship. We have modified the original recommendation to reflect that a substantially complete and signed application provides authorization and there is a need to preserve documentation of the authorization. This recommendation is now the last recommendation of Finding 2.

Recommendation 2.4
Require a lender to report the date of the signed consolidation application during the initial request for access to a borrower's record for which it does not hold any or all of the loans.

FSA Comments
FSA agreed with this recommendation. FSA stated that NSLDS will create a method to collect the date of the signed application on the NSLDS website during the initial request to access a borrower's records when it is indicated that access is required for consolidation purposes.

OIG Response
As noted above, we recommend that FSA require both consolidating and non-consolidating lenders maintain signed applications establishing the business relationship that allows access to NSLDS. We have updated this recommendation to include this requirement for non-consolidating lenders. The recommendation has been renumbered as 2.2.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives for this inspection were to:

1. Evaluate FSA's process for granting NSLDS IDs and passwords to external users except for schools and borrowers, and
2. Determine whether the extent of access FSA provides these external users is appropriate.

We began our fieldwork on July 3, 2007, and conducted an exit conference on December 4, 2007. We reviewed the HEA, applicable regulations, GAO *Standards for Internal Control in the Federal Government*, and OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*. We also reviewed the documentation provided by FSA including the SAIG Enrollment Forms, Department of Education User Participation Request Form, NSLDS System Security Plan, Electronic Announcements regarding Access to NSLDS, Procedures and Framework for Restoring NSLDS Access, Reinstatement Updates, Central Processing System (CPS) Participation Management NSLDS Application Updates, Instructions for NSLDS Users, and the reinstatement materials provided to guaranty agencies, lenders, and state grant agencies.

We interviewed FSA staff from the following offices: NSLDS, Business Operations, Chief Financial Officer, Participation Management, Ombudsman, Student Credit and Management, Policy Liaison and Implementation, Communication and Management Services, and the Office of Program Compliance. We also interviewed Department staff from the Office of the General Counsel and the Office of Postsecondary Education.

To evaluate FSA's process for granting NSLDS IDs and passwords to external users except for schools and borrowers, we met with FSA staff to determine how lenders, guaranty agencies, state agencies, and lenders servicers were classified as eligible external users and how these users applied for NSLDS access.

To determine whether the extent of access FSA provides these external users is appropriate, we determined the information that each entity can access and conducted interviews to establish the type of information needed by each external entity to perform their designated FFEL Program functions.

Our inspection was performed in accordance with the *2005 President's Council on Integrity and Efficiency Quality Standards for Inspections* appropriate to the scope of the inspection described above.

MAY 28 2008

TO: Wanda A. Scott
Assistant Inspector General
Evaluation, Inspection and Management Services
Office of Inspector General

FROM: Lawrence A. Warder
Acting Chief Operating Officer

SUBJECT: Draft Inspection Report – "Review of the Department's Process for Granting Access to the National Student Loan Data System"
Control Number ED-OIG/I13H0006

Thank you for providing us with an opportunity to respond to the Office of Inspector General's (OIG) Draft Inspection Report, "Review of the Department's Process for Granting Access to the National Student Loan Data System" (NSLDS), dated April 14, 2008.

Federal Student Aid is committed to strengthening our internal controls over NSLDS access. As you are aware, the Department of Education (Department) acted quickly to suspend access of external users to NSLDS temporarily in April 2007 when the Department observed a significant increase in usage by certain users. As your report states, we examined NSLDS' access rules to ensure that the privacy rights of borrowers in NSLDS were protected, as required by the Privacy Act of 1974, and that users were accessing NSLDS for authorized purposes only.

Following last year's temporary suspension of NSLDS access, the Department worked aggressively to strengthen its processes and procedures for granting access to NSLDS to ensure only those with a legitimate need have access to the borrower information stored in the NSLDS. As a result, Federal Student Aid developed new controls and implemented new procedures that address many of your report's concerns. That said, we are currently changing NSLDS' access requirements to allow us to further monitor access to NSLDS and identify potential access violations. These new access controls should be fully operational by year's end.

While we agree with the majority of your recommendations, there are several recommendations that we cannot fully implement. We either do not have regulatory or statutory authority or the recommended solution would have unintended consequences if we were to implement the changes as suggested.

For example, the report recommends that the Department develop procedures to evaluate and regulate the adequacy of lender and guaranty agency agreements. While federal regulations at 34 CFR 682.419(b)(19) require a guaranty agency to have a written lender agreement with each lender that participates in the loan guaranty program, the Department's authority is limited to reviewing the lender agreements to ensure they exist and that the agreements do not violate existing regulations. We welcome your guidance on how we can determine the adequacy of the agreements, given the statutory and regulatory limitations.

Our responses to each of the recommendations are discussed in the attachment. Once again, we thank you for the recommendations and the opportunity to review and respond to the report.

Attachment

cc: W. Christian Vierling, Director, Evaluation and Inspection Services

Finding No. 1 – FSA Has Weak Controls over the Process of Assigning Lender Identification Numbers

Recommendation 1.1. Develop written procedures for assigning LIDs, including a standard appeal process.

Response: We agree with this recommendation. In January 2008, we developed and implemented written procedures for assigning LIDs, including a challenge/appeal process.

Recommendation 1.2. Develop procedures to verify and evaluate the adequacy of agreements between the guaranty agency and lender before issuing an LID.

Response: Federal Student Aid does not agree with this recommendation as written. Specifically, under 34 CFR 682.410 (b)(19), a guaranty agency is required to have a written agreement with each lender that participates in the loan program through that GA, and the Department has the authority to review those agreements to ensure they exist. However, the regulations do not have specific standards for those agreements. Therefore, FSA has limited authority to regulate the "adequacy" of the agreements between the guaranty agency and lender beyond the existing statutory and regulatory requirements. Federal Student Aid requests OIG's guidance on how we can determine the "adequacy" of the agreements.

Recommendation 1.3. Develop procedures to verify and evaluate the adequacy of the ELT agreements between the lender and the beneficial holder before issuing an LID.

Response: We do not fully concur with this recommendation. We developed and implemented revised procedures for reviewing ELT agreements between the lender and the beneficial holder before issuing an LID. The revised procedures now require that Federal Student Aid receive copies of the agreements, financial statements, financing plans, and co-signed documents acknowledging the working partnership between the entities. With respect to the evaluation of the adequacy of the ELT agreements, the regulations do not have specific standards for those agreements. Therefore, Federal Student Aid has limited authority to regulate the "adequacy" of the agreements between the lender and the beneficial holder. Federal Student Aid requests OIG's guidance on how we can determine the "adequacy" of the agreements. Upon receipt of guidance from OIG, Federal Student Aid will implement verification procedures.

Attachment-- Draft Inspection Report – "Review of the Department's Process for Granting Access to the National Student Loan Data System (NSLDS)," Control Number ED-OIG/I13H0006

Recommendation 1.4. Obtain and verify current agreements between guaranty agencies and lenders and between lenders and beneficial holders in an ELT arrangement.

Response: Federal Student Aid does not concur with OIG's recommendation as written. Specifically, under 34 CFR 682.410 (b)(19), a guaranty agency is required to have a written lender agreement with each lender that participates in the loan program through that GA, and the Department has the authority to review those agreements to ensure they exist. However, the regulations do not have specific standards for those agreements. Therefore, Federal Student Aid has limited authority to verify the "adequacy" of the agreements between the guaranty agency and lender beyond the existing statutory and regulatory requirements. Federal Student Aid requests OIG's guidance on how we can verify the "adequacy" of the agreements. Upon receipt of guidance from OIG, Federal Student Aid will implement verification procedures.

Finding No 1B: FSA's Process for Granting NSLDS IDs, Passwords, and Access to External Users is Weak

Recommendation 1.5. Clarify and strengthen guidance to Primary Data Point Administrators (DPAs) to ensure their users understand and comply with the rules for NSLDS.

Response: In January 2008, procedures for enrolling users for access to FSA systems through the Student Aid Internet Gateway (SAIG) enrollment process were clarified and strengthened. NSLDS, among other systems, utilizes this method to provide access to external partners DPA responsibilities as well as additional requirements for the Primary DPA and CEO were strengthened and clarified. The signature process was improved to ensure the CEO or proper designee is accountable for the users' access. Additionally, the Federal Student Aid user statement clarified information regarding the appropriate uses of Federal Student Aid systems and the protection of Privacy Act information.

Recommendation 1.6. Develop and implement control procedures, including edit checks, to monitor access to NSLDS, and hold Primary DPAs accountable for unauthorized usage.

Response: We agree to implement control procedures to monitor access to NSLDS. However, FSA disagrees with holding the Primary DPAs accountable for unauthorized usage because we hold the CEO or designee accountable for the user's access. In accordance with GEN 05-06, Federal Student Aid holds the organization as well as individual users responsible.

Attachment-- Draft Inspection Report – "Review of the Department's Process for Granting Access to the National Student Loan Data System (NSLDS)," Control Number ED-OIG/I13H0006

Reports will be made available for Primary DPAs to monitor the usage and potential access violations. We expect to have this completed by December 31, 2008. When the reports are available, we will send the Primary DPAs an email to let them know that the reports are available and inform them that we expect them to use the reports to monitor usage and potential access violations.

Recommendation 1.7. Develop a requirement for all users to certify that they have read and will comply with the rules and authorized users of NSLDS and require external users to obtain application and computer security training prior to initial logon.

Response: We agree with this recommendation. By December 2008, NSLDS will develop a certification page with the rules and authorized uses of NSLDS that users will have to accept at logon to begin to access the NSLDS website. This certification page will also provide a computer security training download component: The user will certify that they read, understood and agreed to the application and security training.

Recommendation 1.8. Strengthen the requirements of the Primary DPAs to ensure that policies and procedures are in place to ensure that new users understand the sensitive nature of the NSLDS and the penalties for the misuse of the system.

Response: We agree with this recommendation. In January 2008, we implemented new procedures that require the Primary DPA to be responsible for obtaining and storing a signed User Responsibility Statement for each user that registers for access to Federal Student Aid systems via the SAIG enrollment process. Additionally, NSLDS now directs all new NSLDS User IDs to the Primary DPA who is responsible for delivery of the User ID and the NSLDS Rules of Behavior to each new user.

Recommendation 1.9. Require external entities to report all internal control weaknesses over NSLDS access to FSA. FSA should evaluate the weaknesses and take the appropriate action to safeguard the system.

Response: We agree with this recommendation. We will provide language to the Office of Inspector General to include this step in the A-133 Lender/Servicer Audit Guides.

Attachment-- Draft Inspection Report – "Review of the Department's Process for Granting Access to the National Student Loan Data System (NSLDS)," Control Number ED-OIG/I13H0006

Finding No 2 – FSA Does Not Ensure that External Users Accessing NSLDS Have an Ongoing Business Relationship with the Borrower

Recommendation 2.1. Develop and implement a process to confirm that lenders, lender servicers, and ELTs have an ongoing business relationship with the borrower before the borrower's record is accessed.

Response: We disagree with this recommendation. The relationship with the borrower begins with the loan application and/or guaranty process. Lenders and servicers need to view data on NSLDS to determine eligibility of a loan or provide proper servicing of FFEL loans to a borrower.

Federal Student Aid believes an alternative recommendation will reduce the inappropriate access. We propose developing a monitoring tool to identify instances of borrower access where no relationship exists or was recently established after records were accessed. We will then contact the institution to request additional information and to determine appropriate next steps. We anticipate having this tool in place by December 2008.

Recommendation 2.2. Modify NSLDS to allow only the loan holding lender and its servicer to view the borrower's summary default view and only those loans that the borrower holds with the individual lender.

Response: We disagree with this recommendation. Lenders and servicers rely on data in NSLDS to grant deferments and forbearances, consolidate loans, and provide customer service to borrowers and schools. By providing only limited information, the lender will not see loan statuses of deferment or forbearance on loans they do not hold. They will also not be able to determine the validity of Loan Verification Certificates or consolidation loan applications. Federal Student Aid recommends that NSLDS create a monitoring tool to identify instances of borrower access where no relationship exists or was recently established after records were accessed.

Recommendation 2.3. Provide a borrower or a prospective borrower the ability to authorize NSLDS to provide one lender access to his or her records for consolidation and counseling purposes for a limited amount of time.

Response: We disagree with this recommendation. It is acceptable for a lender to access a record on NSLDS once it has received a substantially complete, signed consolidation loan application. The loan application signed by the borrower gives the lender permission to access his/her records. Requiring the borrower to authorize access to NSLDS for one lender to view NSLDS negates the permission already provided by the loan application. Further, it places an additional burden on the borrower.

Attachment-- Draft Inspection Report – "Review of the Department's Process for Granting Access to the National Student Loan Data System (NSLDS)," Control Number ED-OIG/I13H0006

Recommendation 2.4. Require a lender to report the date of the signed consolidation application during the initial request for access to a borrower's record for which it does not hold any or all of the loans.

Response: We agree with this recommendation. NSLDS will create a method to collect the date of the signed application on the NSLDS website during the initial request to access a borrower's records when it is indicated that access is required for consolidation purposes.