



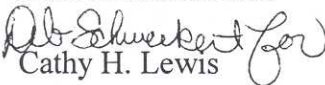
UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE INSPECTOR GENERAL

AUG 1 2005

INSPECTION MEMORANDUM

To: Theresa S. Shaw
Chief Operating Officer
Federal Student Aid

From: 
Cathy H. Lewis
Assistant Inspector General
Evaluation, Inspection, and Management Services

Subject: Inspection of Access to the National Student Loan Data System (NSLDS)
(ED/OIG I13F0004)

This memorandum provides the results of our inspection of the Security Plan for the Department of Education's (Department) National Student Loan Data System (NSLDS) and its compliance with Departmental Information Technology (IT) policies. Our inspection objectives were to determine (1) whether the security rules and procedures in the NSLDS Security Plan comply with the Department's *Handbook OCIO-1, Handbook for Information Technology Security Policy* (ED IT Security Policy) and its supplements, and (2) whether contractor employees who have user access to NSLDS have the appropriate security clearances as required in the NSLDS Security Plan.

Executive Summary

The NSLDS Security Plan provides the scope, objectives, controls, and staff responsibilities for the NSLDS system's security. As with all Department-owned IT systems, the NSLDS Security Plan must comply with the *Handbook OCIO-1, Handbook for Information Technology Security Policy* (ED IT Security Policy)¹ and its supplements, including the *Information Technology Security Controls Reference Guide* (IT Security Controls Reference Guide) and the *Information Technology Security Awareness and Training Program Plan* (IT Security Training Program Plan). We found five areas where the NSLDS Security Plan does not comply with the requirements stated in the ED IT Security Policy and its supplements. The plan does not provide a timeline for completing new contractor employee orientation on security policy awareness, does not include requirements for recertification for user accounts, does not follow Department policy on content and duration for passwords, does not require weekly review of audit logs, and does not include account termination procedures for all users. We also determined that not all

¹ 1.2, ED IT Security Policy.

contractor employees with user access to NSLDS have appropriate security clearances as required by the NSLDS Security Plan.

Background

Section 485B of the Higher Education Act (HEA) of 1965 as amended requires the implementation of a National Student Loan Data System (NSLDS). Implemented in 1993, 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 (GAs), 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)/supplemental PCA, Credit Reform Act support, and preparation of financial aid transcript information.²

Applied Engineering Management (AEM), a contractor, currently provides support to FSA for the operation of NSLDS. AEM's duties include maintaining and implementing the NSLDS Security Plan. Under the terms of its contract with FSA, AEM is obligated to fulfill all of the functions and procedures specified in the NSLDS Security Plan. FSA is responsible for providing oversight and ensuring that the security procedures, as written, are fulfilled by AEM.

Inspection Results

Objective 1: Determine whether the security rules and procedures in the NSLDS Security Plan comply with the Department's ED IT Security Policy.

The *Handbook OCIO-1, Handbook for Information Technology Security Policy* (ED IT Security Policy) describes the overall information technology (IT) security policy for the Department of Education (Department) and provides guidance for implementing the Department's IT security regulations. Its supplements include the *Information Technology Security Controls Reference Guide* (IT Security Controls Reference Guide) and the *Information Technology Security Awareness and Training Program Plan* (IT Security Training Program Plan). The NSLDS Security Plan must comply with the ED IT Security Policy and its supplements.³ The NSLDS Security Plan provides an overview of the security requirements of the system and identifies existing or planned controls to meet those requirements. It also establishes the responsibilities and appropriate behavior of individuals who access NSLDS.

Our review showed that there are five areas in which the NSLDS Security Plan does not comply with ED IT Security Policy and its supplements.

² Office of the Inspector General, Final Audit Report: NSLDS Can Be Enhanced if Loan Principal and Interest Balances and Statutes are Updated With Lender Data. 09/1998.

³ Section 1.2, ED IT Security Policy

Training

The IT Security Training Program Plan, which is a supplement to the ED IT Security Policy, requires that the Department provide “an awareness briefing as part of employee orientation within 60 days from date of hire.”⁴ The NSLDS Security Plan does not include a written timeline for new contractor employees for NSLDS to receive this type of training.⁵ According to AEM, new employees receive security training within three days of hire. However, a timeline for providing the required awareness briefing needs to be included in the plan to be consistent with Department policy.

Recertification

The IT Security Controls Reference Guide, which is a supplement to the ED IT Security Policy, states that, “user account recertification must be performed at least annually to identify and remove users who have left the organization or whose duties no longer require access to a specific system resource. Recertification provides a secondary method of ensuring that all user accounts are valid and authorized.”⁶ The NSLDS Security Plan does not state any requirement for a recertification process.⁷

FSA staff stated that although the NSLDS Security Plan does not include recertification procedures, they reconcile staffing records from human resources with their master list of internal⁸ user accounts in order to remove users who no longer need access. During our inspection, FSA asked the Virtual Data Center (VDC) to run a report of all internal and external⁹ users who have inactive¹⁰ NSLDS UserIDs. The report showed that NSLDS had a total of 11,199 inactive UserIDs that were not in a \$DEL group.¹¹ The report included UserIDs that were last used as far back as November 11, 1993. The breakdown of inactive UserIDs not placed in a \$DEL group, as identified in that report, is as follows:

⁴ Section 1, IT Security Training Program Plan.

⁵ 3.9, NSLDS Security Plan (April 2005 Preview). 03/05/2004.

⁶ 4.1.1, IT Security Controls Reference Guide. Account termination procedures are the primary method for removing users.

⁷ During our interviews, FSA stated that it is formulating a written recertification policy and that it is also considering extending its recertification efforts to include contractor employees.

⁸ Department and Contractor Employees are considered internal users.

⁹ External users include users at schools, GAs, lenders, and state agencies.

¹⁰ Inactive IDs are UserIDs that have not been used to access NSLDS for 365 days or more.

¹¹ A UserID that is in a \$DEL group or in delete status can no longer access the system because the RACF (see Footnote 12) or system access is turned off. However, UserIDs are never permanently deleted, but are retained for audit trail purposes.

User Group	No. of Inactive UserIDs	Oldest Date of Last Login
Department Employees	47	July 7, 2003
Contractors	668	November 11, 1993
NSLDS Trainer	231	January 6, 2000
Guaranty Agencies	462	January 28, 1999
Lender/Lender Servicers	1,105	October 25, 2000
School/School Servicers	8,671	May 22, 1996
State Agencies	15	January 15, 2002

FSA stated that on December 22, 2004, it discussed with AEM the deletion of inactive UserIDs. AEM provided a step-by-step plan for placing inactive UserIDs into delete status. FSA also stated that on February 3, 2005, it requested that VDC place all Department and contractor employees who had not accessed NSLDS in the last twelve months into deleted status on a monthly basis.

At our exit conference on March 28, 2005 FSA indicated that all of the 11,199 UserIDs on the inactive UserID list had already been deleted and that their Resource Access Control Facility (RACF)¹² access had been turned off. In a phone interview with VDC on March 30, 2005, however, VDC indicated that, as of that morning, all of the 11,199 users on the inactive UserID list were not in \$DEL groups and could gain access to the system if their passwords were reset by the Customer Service Center (CSC). VDC then stated that it received instructions from FSA on March 29, 2005 to place all UserIDs on the inactive UserID list into \$DEL groups. In a subsequent interview, FSA confirmed that the contractor had not put the 11,199 UserIDs into delete status by March 28, 2005 as reported during the exit conference.

Although FSA and its contractors discussed the deletion of inactive UserIDs on December 22, 2004, FSA did not follow up with AEM and VDC to ensure that the inactive UserIDs were subsequently placed into \$DEL groups. Due to FSA's lack of oversight in verifying that the contractors fulfill their assigned tasks, FSA inaccurately reported at the exit conference that the UserIDs were in delete status. Although the inactive UserIDs are now in \$DEL groups,¹³ FSA still needs to add language to the NSLDS Security Plan that reflects the Department's requirement for an annual recertification process.

Password Controls

The ED IT Security Policy requires that passwords to IT systems have a "minimum of 8 alphanumeric characters" and must have a "maximum password age of 90 days."¹⁴ The Office of Inspector General's FY 2004 Federal Information Security Management Act (FISMA) Audit Report found that the NSLDS password controls do not comply with the ED IT Security Policy.

¹² RACF is a security system that provides functions to identify and verify system users, define system resources, authorize the users who need access to protected resources, control the means of access to protected resources, and log system violations and unauthorized attempts to gain access to the system.

¹³ VDC confirmed that on March 30, 2005 it placed the 11,199 inactive UserIDs into delete status.

¹⁴ 2.3.4, ED IT Security Policy. See also 4.1.2, IT Security Controls Reference Guide.

According to the NSLDS Security Plan, passwords may be six to eight alphanumeric characters and are valid for 120 days.¹⁵ At the time of our review, the NSLDS password aging timeframe was 120 days. According to FSA, on March 18, 2005 VDC changed the password aging timeframe to 90 days, after our fieldwork had been completed. We have confirmed that FSA implemented the password change, but this change still has not been incorporated into the Security Plan.

Audit Trails

The ED IT Security Policy states, “Principal Offices must ensure that system log records are reviewed at a minimum on a weekly basis.”¹⁶ The NSLDS Security Plan states that audit trails, which are synonymous with system log records, are reviewed on an “as-needed basis,”¹⁷ which is inconsistent with the Department’s requirement. The plan also does not specify who is responsible for these reviews. During our entrance conference, FSA staff stated that the contractor, AEM, is responsible for preparing and reviewing these records. They referred us to the contractor to determine how often AEM performs these functions. AEM and its subcontractors stated that they do not regularly prepare or review these records, and in fact AEM was not aware that it was responsible for doing so. As a result, neither FSA nor AEM is regularly producing audit trails for review. Audit trails are critical to identifying possible security violations. The language in the NSLDS Security Plan needs to be modified to be consistent with the Department’s ED IT Security Policy.

Account Termination Procedures

The IT Security Controls Reference Guide states, “all user accounts are to be disabled within 24 hours of the employee’s separation from the Department, or immediately in the event of an unfriendly termination.”¹⁸ Although the NSLDS Security Plan states that there is a documented process for closing all user accounts,¹⁹ the plan only includes written account termination procedures for contractor employees.²⁰ The plan does not include account termination procedures for Department employees.²¹ AEM and FSA employees confirmed that the documented process for closing user accounts is currently being applied only to contractor employees. The NSLDS Security Plan needs to be modified to accurately reflect the requirements of the Department’s IT Security Controls Reference Guide.

¹⁵ 4.1.2.2, NSLDS Security Plan (April 2005 Preview), 03/05/2004.

¹⁶ 2.3.6.2, ED IT Security Policy. See also 4.5.3, IT Security Controls Reference Guide.

¹⁷ 4.4.1, NSLDS Security Plan (April 2005 Preview), 03/05/2004.

¹⁸ 4.1.1, IT Security Controls Reference Guide

¹⁹ 3.1.1.6, NSLDS Security Plan (April 2005 Preview), 03/05/2004.

²⁰ 3.1.1.8, NSLDS Security Plan (April 2005 Preview), 03/05/2004.

²¹ In response to our request for written account termination procedures for Department employees, FSA provided handwritten procedures on notebook paper.

Recommendations

Based upon the results of our inspection, we recommend that the Office of Federal Student Aid (FSA):

1. Amend the NSLDS Security Plan as follows to comply with the ED IT Security Policy:
 - a. Provide a written timeline for new contractor employees to receive an IT awareness briefing;
 - b. Include at least annual recertification procedures to identify and remove access of internal users who have left the organization, current employees whose duties no longer require NSLDS access, and users who have not accessed the system for a specified period of time;
 - c. Extend minimum password length to eight alphanumeric characters and ensure that the recently updated 90-day password aging timeframe is included;
 - d. Include language requiring that system log records are reviewed on at least a weekly basis and clarify with AEM its responsibility for ensuring that it is conducting these reviews; and
 - e. Incorporate written, formalized policy on account termination procedures for Departmental employees.

2. Improve oversight of contractor responsibilities and verify that contractors fulfill assigned tasks as directed.

Objective 2: Determine whether contractor employees who have user access to NSLDS have the appropriate security clearances as required in the NSLDS Security Plan.

The NSLDS Security Plan requires all contractor employees²² to have the security clearance required for their positions.²³ Not all NSLDS contractors, however, have the appropriate clearance.

The NSLDS Security Plan requires that all High Risk contractor employees have a 6C²⁴ security clearance and all Moderate Risk contractor employees have a 5C²⁵ security clearance. Upon comparing the contractor roster of 5C and 6C employees to the contractor security clearance records from the Office of Personnel Security, we discovered that not all of the contractor employees in Moderate and High Risk positions have the appropriate security clearances

²² Includes all VDC, AEM, and subcontractor employees with Pearson Government Solutions and Briefcase.

²³ 3.1, NSLDS Security Plan (April 2005 Preview), 03/05/2004.

²⁴ High Risk employees require 6C clearances and may not work in a High Risk position until their preliminary security screenings are complete and the results approved by ED. If the employee's security clearance is pending, he or she must be denied access to High Risk material until the investigation is complete and the results approved by ED. Employees in High Risk Level positions are able to access a system during its operation or maintenance in a manner that entails high risk of grave damage, or of realizing significant personal gain (OM:5-101, Contractor Employee Personnel Security Screenings).

²⁵ Moderate Risk employees require 5C security clearances and may begin work in their position upon submittal of their paperwork. Employees who hold 5C level positions have the potential for moderate to serious impact because their duties are of considerable importance to the agency mission and their duties require individuals to view or use Privacy-Act protected information. A higher authority staff member who works in a High Risk Level position reviews the work of moderate risk employees. (OM:5-101, Contractor Employee Personnel Security Screenings).

required for their positions. The following is a breakdown of the security clearance statuses for the 99 NSLDS contractor employees as of April 8, 2005:

- Seventy-four contractor employees have the correct security clearance for their position sensitivity level.
- Fourteen contractor employees in Moderate Risk Level positions have only 1C security clearances when their positions require 5C clearances; there is no pending request for 5C clearances.
- Seven contractor employees in Moderate Risk Level positions have not turned in any paperwork to request a security clearance.
- Three contractor employees in High Risk Level positions have only 5C security clearances when their positions require 6C clearances; there is no pending request for 6C clearances for these individuals.
- One contractor employee in a High Risk Level position has not turned in any paperwork to request a security clearance.

We identified that 25 of the 99 NSLDS contractor employees do not have the security clearances required by their position's sensitivity level, as required by the NSLDS Security Plan and OM:5-101, Contractor Employee Personnel Security Screenings. It is the responsibility of FSA to provide oversight to ensure that AEM verifies that contractor employees have appropriate security clearances;²⁶ however, this provision of the NSLDS Security Plan is not currently being followed.

Recommendations

Based upon the results of our inspection, we recommend that the Office of Federal Student Aid (FSA):

3. Ensure that contractor employees have the appropriate security clearance for their position and that the 25 contractor employees without proper clearance immediately obtain security clearances.
4. Ensure that contractor employees in High Risk Level Positions not granted a preliminary clearance are denied access to High Risk material until they receive a preliminary clearance.

Objectives, Scope, and Methodology

The objectives of our inspection were to:

1. Determine whether the security rules and procedures in the NSLDS Security Plan comply with the Department's ED IT Security Policy.
2. Determine whether contractor employees who have user access to NSLDS have the appropriate security clearances as required in the NSLDS Security Plan.

²⁶ 3.1, NSLDS Security Plan (April 2005 Preview), 03/05/2004.

We began our primary fieldwork December 9, 2004 and concluded it on February 15, 2005. We focused our inspection on the compliance of the April 2005 Preview Copy of the NSLDS Security Plan, received on December 16, 2004, with Departmental IT policies. We compared the NSLDS Security Plan to the policies set forth in the ED IT Security Policy. We also reviewed the implementation of the NSLDS Security Plan rules regarding contractor security clearances.

We interviewed NSLDS Department and contractor staff. We obtained the master list of Department and contractor employees who have NSLDS UserIDs. We also obtained other contract documents including the Statement of Objectives and the list of contract deliverables. We used these documents and Departmental policies to determine if the contractor was following requirements of the NSLDS Security Plan.

FSA provided us with a list of all inactive NSLDS UserIDs that had not been permanently deleted. VDC ran this report for FSA on February 4, 2005. We divided the list by user group and determined the oldest date of the last login for each user group.

To determine whether contractors had the appropriate security clearances required for their positions, we requested a list of all 5C and 6C contractor employees from the FSA staff. We received this roster on January 10, 2005, which included the 99 contractor employees who are required to have 5C or 6C security clearances depending on their position sensitivity level. We compared this roster of employees to the contractor security clearance records obtained from the Office of Personnel Security (OPS) on January 13, 2005. On April 8, 2005, we obtained updated contractor security clearance records from OPS.

The inspection team also requested a copy of audit trails reviewed by the contractor staff during August and October 2004. Neither FSA nor the contractor could produce these documents during our inspection.

Department Response

We provided FSA with a draft report. FSA's comments and our responses are presented below. The complete FSA response is included as an addendum to this report.

Recommendations

- 1. Amend the NSLDS Security Plan to provide a written timeline for new contractor employees to receive an IT awareness briefing; to include at least annual recertification procedures to identify and remove internal users who have left the organization, current employees whose duties no longer require NSLDS access, and users who have not accessed the system for a specified period of time; to extend minimum password length to eight alphanumeric characters and ensure that the recently updated 90-day password aging timeframe is included; to include language requiring that system log records are reviewed on at least a weekly basis; and to incorporate written, formalized policy on account termination procedures for Department employees.**

Finding 1: The NSLDS Security Plan does not comply with the ED IT Security Policy and its supplements in five areas: Training, Recertification, Password Controls, Audit Trails, and Account Termination Procedures.

FSA Comments: FSA agrees with this recommendation and will modify the System Security Plan (SSP) as recommended. The password length and 90-day password aging items were identified during the Certification and Accreditation process for the VDC (POA&M VDC-228 and VDC-229) and these items have been implemented for NSLDS. This change will appear in the next scheduled SSP deliverable in April 2006. Additionally FSA stated that the OIG suggested that NSLDS permanently delete inactive UserID's. According to FSA, the NSLDS policy is to place inactive users in a delete status, thereby removing access.

OIG Response: No change has been made to the recommendation. In the draft report, we used the term "permanently delete" to refer to placing inactive UserIDs in a delete status. We have clarified the terminology used in the report.

2. Improve oversight of contractor responsibilities and verify that contractors fulfill assigned tasks as directed.

FSA Comments: FSA agrees and has improved its oversight of contractor's performance of NSLDS security. We are performing reviews of the weekly project plan and deliverables to ensure immediate identification of issues and appropriate resolution.

OIG Response: No change has been made to the recommendation.

3. Ensure that contractor employees have the appropriate security clearance for their position and that the 25 contractor employees without proper clearance immediately obtain security clearances.

Finding 2: Not all NSLDS contractor employees have the appropriate clearance.

FSA Comments: FSA agrees with the recommendation and will develop guidelines to ensure that contractor staff has appropriate security clearances for their positions. NSLDS has identified the 25 contractor employees without proper security clearance. As of July 7, 2005, all contractor employees have submitted appropriate clearance paperwork, or their access to NSLDS was revoked.

OIG Response: No change has been made to the recommendation.

4. Ensure that contractor employees in High Risk level positions not granted a preliminary clearance are denied access to High Risk material until they receive a preliminary clearance.

FSA Comments: FSA agrees. NSLDS provided instructions to its contractor regarding High Risk level positions and access rights on June 27, 2005, and validated that the contractor is in compliance with these instructions. Procedures will be incorporated into the annual updates to the NSLDS Security Plan scheduled for April 2006.

OIG Response: No change has been made to the recommendation.

Administrative Matters

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.

We appreciate the cooperation given to us during the inspection. If you have any questions or wish to discuss the contents of this report, please call Deb Schweikert, Director, Evaluations and Inspections Division at 202-245-7026. Please refer to the control number in all correspondence relating to this report.



**F E D E R A L
S T U D E N T A I D**
We Help Put America Through School

CHIEF OPERATING OFFICER

JUL - 8 2005

TO: Cathy H. Lewis
Assistant Inspector General
Evaluation, Inspection, and Management Services

FROM: Theresa S. Shaw *TSS*
Chief Operating Officer

SUBJECT: Draft Inspection Memorandum
Inspection of Access to the National Student Loan Data System (NSLDS)
ED-OIG/ I13-F0004

This is in response to your June 6, 2005, Draft Inspection Memorandum. In general, FSA agrees with the OIG findings and recommendations. The following responses address the referenced findings and recommendations in the memorandum.

Finding 1: The NSLDS Security Plan does not comply with the ED IT Security Policy and its supplements in five areas: Training, Recertification, Password Controls, Audit Trails, and Account Termination Procedures.

Recommendation 1: Amend the NSLDS Security Plan to provide a written timeline for new contractor employees to receive an IT awareness briefing; to include at least annual recertification procedures to identify and remove internal users who have left the organization, current employees whose duties no longer require NSLDS access, and users who have not accessed the system for a specified period of time; to extend minimum password length to eight alphanumeric characters and ensure that the recently updated 90-day password aging timeframe is included; to include language requiring that system log records are reviewed on at least a weekly basis; and to incorporate written, formalized policy on account termination procedures for Department employees.

FSA Response: FSA identified the password length and 90-day password aging items during the Certification and Accreditation process for the VDC (POA&M VDC-228 and VDC-229). These items have been implemented for NSLDS. FSA agrees with this recommendation and will modify the System Security Plan (SSP) as recommended. The update will appear in the next scheduled SSP deliverable in April 2006.

Recommendation 2: Improve oversight of contractor responsibilities and verify that contractors fulfill assigned tasks as directed.

FSA Response: FSA agrees and has improved its oversight of contractor's performance of NSLDS security. We are performing reviews of the weekly project plan and deliverables to ensure immediate identification of issues and appropriate resolution.

Finding 2: Not all NSLDS contractor employees have the appropriate clearance.

Recommendation 3: Ensure that contractor employees have the appropriate security clearance for their position and that the 25 contractor employees without proper clearance immediately obtain security clearances.

FSA Response: FSA agrees with the recommendation and will develop guidelines to ensure that contractor staff has appropriate security clearances for their positions. NSLDS has identified the 25 contractor employees without proper security clearance. As of July 7, 2005, all contractor employees have submitted appropriate clearance paperwork, or their access to NSLDS was revoked.

Recommendation 4: Ensure that contractor employees in High Risk level positions not granted a preliminary clearance are denied access to High Risk material until they receive a preliminary clearance.

FSA Response: NSLDS provided instructions to its contractor regarding High Risk level positions and access rights on June 27, 2005, and validated that the contractor is in compliance with these instructions. Procedures will be incorporated into the annual updates to the NSLDS Security Plan scheduled for April 2006.

Additional FSA Response: The OIG suggested that NSLDS permanently delete inactive UserID's; however, it is not NSLDS' policy to permanently delete UserID's. By doing so, we lose the audit trail of the users in our system. The NSLDS policy is to place inactive users in a delete status, thereby removing access.

If you have any questions, you may contact Pamela Eliadis, Director, NSLDS Data Systems Group at (202) 377- 3554.