Statement of
Lorraine Lewis
Inspector General
U.S. Department of Education

Before the
Subcommittee on Oversight and Investigations
Committee on Education and the Workforce
U.S. House of Representatives

September 19, 2000

Mr. Chairman and Members of the Subcommittee:

I am here today at your invitation to discuss matters related to financial management and computer security at the Department of Education. Specifically, I will address: (1) the Department's progress on fiscal year (FY) 1999 financial statement audit recommendations; (2) the status of the FY 2000 financial statement audit; (3) a summary of duplicate payments made in FY 2000; (4) recent OIG computer security reviews; and (5) recent investigations.

Progress on FY 1999 Financial Statement Audit Recommendations

On March 1, 2000, we testified before the Subcommittee on Oversight and Investigations and reported that a total of 139 recommendations had been made for the FY 1995 through the FY 1999 financial statement audits. At that time, 111 recommendations remained open, 28 were closed, and 74 were non-repetitive. Since that hearing, the Department provided us with a response to the FY 1999 financial statement audit and corrective action plans for all of the financial statement audits.

Through the cooperative efforts of the Department and my office, 95 recommendations have closed and 44 remain open. Thirty of the 44 recommendations open for corrective action are non-repetitive. Of the 24 recommendations contained in the FY 1999 financial statement audit, 18 are open and six are closed.

The Department provided my office with updated corrective action plans for the FY 1995 through FY 1999 financial statement audits on September 15, 2000. Currently, we are assessing these corrective action plans.

Fiscal Year 2000 Financial Statement Audits

As a result of meeting the March 1, 2000, deadline for the FY 1999 audit, we are much further along in the audit of FY 2000 than we were this time last year for FY 1999. Timely reporting for FY 1999 has allowed us to plan earlier for this year's audit, with the greatest strides made in the coordination of our own systems audit efforts with those of Ernst & Young's information systems auditors. This coordination has helped increase the audit coverage in this important area of work.

The Department has focused earlier on the financial statement preparation process. For example, the Department prepared two sets of interim statements, as of March 31 and June 30. The final financial statements are due to us on December 1. As Ernst & Young will testify, we are unable to forecast or speculate as to the ultimate opinion which will be rendered in March 2001.

Duplicate Payments

At your request, I am providing this summary of duplicate payments issued by the Department in FY 2000. Four instances of duplicate payments occurred in FY 2000 and involved either grants or student financial assistance. Three of these instances were discovered soon after they occurred by the grantees or schools and the Department was subsequently informed. The other instance was identified by system controls in the electronic payment system.

Two of the instances occurred in October 1999 and two occurred in December 1999. In October, a payment for $19 million was transmitted twice, then subsequently recovered by an electronic reversal. A second instance resulted in $125 million in duplicate payments being issued to approximately 48 grantees. In December 1999, duplicate payments totaling $663,472 were issued to 51 schools, and $6 million was issued to one school. All of these duplicate payments have been recovered.

Computer Security

Several recent OIG reports indicate that the Department needs to improve its computer security controls.

Report on Security Posture, Policies, and Plans

In February 2000, we issued an audit that reviewed the security posture, policies and plans for the Department's 14 mission-critical information technology systems. Our objective was to determine the existence of required security documentation and its compliance with applicable requirements of the Computer Security Act [40 U.S.C. 1441 note], Paperwork

Reduction Act [44 U.S.C. 3506(g)(1)], and Appendix III of the Office of Management and Budget's (OMB) Circular A-130. Specifically, we determined whether these systems had security plans in place, met requirements for a current security review, and had corrective action plans in place to correct identified deficiencies. We also determined whether the Department took steps to screen appropriate personnel and whether system security officers received security training. Our scope did not include a security review of the remaining 161 systems that the Department identifies as non-critical.

During this review, we found the following weaknesses: (1) the Department has not completed revisions of its security policies; (2) systems security officers of student financial assistance systems do not report to managers that have functional authority over the process being automated; (3) security plans are not in place for six mission-critical systems; (4) the Department did not complete required security reviews for six mission-critical systems; (5) there is no process to ensure resolution of identified security deficiencies; (6) many employees responsible for overseeing computer security lack required technical security training; (7) the Department has not taken steps to ensure that appropriate personnel are screened. Two of these findings -- the lack of security plans and the lack of technical security training -- represent noncompliance with the Computer Security Act. All seven findings represent noncompliance with the OMB Circular A-130. Because the Department is not adhering to requirements in Circular A-130, it may not be in compliance with the Paperwork Reduction Act.

The Department agreed with the overall content of our report and concurred with the seven findings. The Chief Information Officer (CIO) recently informed us that the security reviews have now been completed for the remaining six systems and that security plans should be in place for all critical systems by October 2000. The CIO has also updated its IT security

policy and submitted it for clearance as a Department directive. In July, the Deputy Secretary issued a memorandum requiring all Department staff to complete computer security awareness training. According to the Department, as of September 13, 2000, 85 percent of Department staff have completed this training. The CIO is also working to identify individuals who need more specialized training and to acquire the appropriate courses for these staff. As we recommended, the Department also reported security management as a material weakness in its 1999 Federal Managers' Financial Integrity Act report. We will continue to monitor the Department's corrective actions to address our findings and recommendations, as well as conduct an annual review of the Department's security program.

Reviews of GAPS and EDNet

We have also performed detailed security audits of two critical systems in the Department -- the Grant Administration and Payment System (GAPS) and the Department-wide network (EDNet). The review of GAPS security was completed in September 1998. The report *Review of EDNet Security* was completed in July 2000 and evaluated the security posture of the Department's information technology infrastructure. The EDNet is the Department's primary network facility and is comprised of a telecommunications system and many connected resources, including large computers, printers, and local area networks (servers). Use of EDNet allows connectivity among all Departmental information technology resources.

We identified several areas in these audits where the Department can strengthen controls to enhance overall accountability and control of these systems. We cannot disclose the specific findings and recommendations to the public since these audits contain sensitive security-related

information. The Department concurred with our findings and recommendations and we will continue to monitor the progress of their corrective actions.

Review of PDD 63

Our office also recently completed work on an audit entitled *Review of Planning and Assessment Activities for Presidential Decision Directive 63 – Critical Infrastructure Protection*. Presidential Decision Directive 63 (PDD 63) is a national effort to assure the security of the nation's critical infrastructures. We are participating in a government-wide review by the President's Council on Integrity and Efficiency on implementation of PDD 63. Our current audit represents the first phase of this project. The objective for the first phase was to assess the adequacy of agency planning and assessment activities for protecting their critical, cyber-based infrastructures. We reviewed: (1) the adequacy of the Department's plans; (2) its asset identification efforts; and (3) initial vulnerability assessments. We found that the Department needs to revise and implement its critical infrastructure protection plan, identify its critical infrastructure assets, and conduct vulnerability assessments of those assets. Overall, we made ten recommendations to the Department that address our findings. The Department has concurred with our findings and recommendations and we will monitor the progress of their corrective actions.

Recent Actions

Among those actions already implemented, the Department's CIO designated a Deputy CIO for Information Assurance and assigned three additional staff members to the IT security area. The Department has also established the Information and Critical Infrastructure Assurance

Steering Committee (Steering Committee). Its mission is to advise the Deputy Secretary, CIO, and Chief Infrastructure Assurance Officer on Department-wide IT security and critical asset assurance policies and to coordinate and help implement the Department's information security and critical information structure assurance program. The Committee is co-chaired by Deputy Secretary Frank Holleman and CIO Craig Luigart. Senior officers have designated principal office representatives.

The Steering Committee has established several work groups to assist with: (1) security awareness and training, (2) incident handling, (3) background investigations, (4) continuity of operations in case of disaster, (5) authentication and public key infrastructure, (6) privacy protection, and (7) development and implementation of a Department-wide Critical Infrastructure Protection Plan. The CIO has informed us that the Department has established an interagency agreement to use the General Services Administration's *Safeguard Program* to seek contractual support for identifying critical infrastructure assets by December 2000 and perform vulnerability assessments by April 2001. The CIO has informed us that he expects to submit a revised critical infrastructure protection plan to the Steering Committee in October 2000.

These audits reflect the need for improved computer security at the Department. We have identified improvement of computer security posture, policies, and plans as a top management challenge and we will continue to closely monitor the Department's corrective actions on our existing audits. Additionally, we plan to conduct an annual review of the Department's computer security program.

Investigations

As your staff requested verbally, I am providing information on pending investigations. Since the investigations are ongoing, I am providing only the information that is publicly available through court filings or other public disclosures.

Investigation 1

We are conducting a vigorous investigation of individuals who, between 1997 and 1999, purchased equipment with federal funds for non-business related purposes, billed the Department for hours not worked, and received goods purchased with federal funds for personal use. These items include computers, printers, computer software, scanners, cordless telephones, a 61-inch television, walkie-talkies, compact disc players, and other equipment. The total cost of these items to the Department was over $300,000. In addition, it is estimated that between January 1, 1997, and November 30, 1999, approximately $634,000 in unworked hours were fraudulently charged to the Department by individuals involved in the case. Thus far, three individuals, Robert J. Sweeney, Joseph Dennis Morgan, and Raymond L. Morgan, Jr. have pled guilty based on their involvement in the case.

Additionally, the U.S. Attorney's Office for the District of Columbia has filed criminal charges against three other individuals associated with this criminal activity. These three individuals are current employees of the Department who have been placed on indefinite suspension without pay.

Investigation 2

On this matter, I can discuss only what has been made a matter of public record by the filing of a civil complaint to recover fraudulently misdirected Impact Aid funds. My office and the FBI are conducting a vigorous investigation, in conjunction with the U.S. Attorney's Office for the District of Columbia.

On July 13, 2000, the Department of Justice filed a verified civil complaint for forfeiture *in rem* to recover $1,657,980 from several bank accounts, two vehicles, and a building in Riverdale, Maryland. After serving the appropriate interested parties, publishing required notices and waiting the required periods during which time no answers or claims were filed, the Department of Justice filed a motion for default judgment of forfeiture, which is pending before the U.S. District Court for the District of Columbia.

Background information set forth in the complaint states that $1.9 million in Impact Aid grant funds were fraudulently wired into two bank accounts. These Impact Aid funds should have been disbursed to two school districts in South Dakota. Nearly all the funds and property purchased with these funds have been seized by the United States. A *lis pendens* has been placed against the real property. The cars were located and seized in April and May 2000 by OIG, FBI, and local police in Maryland.

Conclusion

Our support for strong financial management and computer security is evidenced by the audits and investigations discussed above. In addition, we will continue to identify areas for improvement at the Department of Education.

Ultimately, the design and implementation of any internal control must be based on an analysis of costs and benefits. Even well designed and implemented internal controls cannot provide absolute assurance against fraud, waste, and abuse. There will always be factors such as human mistakes and acts of collusion that will be outside the control or influence of management. That is why we need to remain vigilant and maintain a credible deterrence through, among other things, a regular program of management reviews, an active hotline function, and vigorous audit, investigative, and inspection operations.

Mr. Chairman, that concludes my prepared testimony. I am happy to answer any questions you or other members of the Subcommittee may have on these issues.