REPORT NO. 2012-027
NOVEMBER 2011

DEPARTMENT OF EDUCATION

CASH ADVANCE AND REPORTING OF DISBURSEMENTS SYSTEM (CARDS)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

STATE BOARD OF EDUCATION

Pursuant to Article IX, Section 2 of the State Constitution and Section 20.15, Florida Statutes, the State Board of Education supervises the system of free public education and is the head of the Department of Education. The Board members who served during the period of audit were:

Kathleen Shanahan, Chair	
T. Willard Fair, Chair	Through March 22, 2011
Roberto Martinez, Vice Chair	
Gary Chartrand	From May 16, 2011
Dr. A. K. Desai	
Barbara S. Feingold	From July 18, 2011
Mark Kaplan	Through July 20, 2011
John R. Padget	
Susan Story	Through December 31, 2010

COMMISSIONER OF EDUCATION

The State Board of Education appoints the Commissioner of Education, who serves as the Executive Director of the Department of Education. The Commissioners who served during the period of audit were:

Dr. Eric J. Smith	November 30, 2007, through June 10, 2011
John Winn, Interim	June 11, 2011, through July 30, 2011
Gerard Robinson	From July 31, 2011

The audit team leader was Hilda S. Morgan, CPA, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF EDUCATION

Cash Advance and Reporting of Disbursements System (CARDS)

SUMMARY

The Bureau of the Comptroller within the Department of Education (Department) is responsible for the fiscal budgeting and reporting of State and Federal funds that have been awarded, or are available for distribution, as grants to subgrantees within the educational community. The Cash Advance and Reporting of Disbursements System (CARDS) was established to provide users with information on the financial status of projects that have been awarded Federal funds.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to CARDS. The results of our audit are summarized below:

CASH MANAGEMENT

Finding No. 1: The Department did not have written procedures and had not implemented processes for monitoring subgrantee cash on hand from Federal cash advances and for subgrantee calculation and remittance of interest earned on cash advances.

SECURITY CONTROLS

Finding No. 2: The access privileges of some employees and contractors to CARDS and related IT resources were not appropriate for their job responsibilities and did not enforce an appropriate separation of incompatible duties.

Finding No. 3: The Department did not timely disable the CARDS access privileges of two former employees.

Finding No. 4: The Department's CARDS access authorization forms were not reflective of the actual CARDS access privileges that had been granted to some employees. Additionally, the access authorization form for one Department employee included in our sample lacked the approval signature of the employee's supervisor.

Finding No. 5: Contrary to the requirements of the State of Florida, *General Records Schedule,* for the retention of access control records, the Department did not retain complete access control records for CARDS.

Finding No. 6: Certain security controls related to user authentication needed improvement.

BACKGROUND

The Commissioner of Education is the chief educational officer of the State and is responsible for operating all Statewide functions necessary to support the State Board of Education, including strategic planning and budget development, general administration, assessment, and accountability. Additionally, the Commissioner is responsible for developing and implementing a plan for cooperating with the Federal Government in carrying out any or all phases of the educational program and to recommend policies for administering funds that are appropriated by Congress and apportioned to the State for any and all educational purposes.

The Department developed CARDS to provide users with information on the financial status of projects that have been awarded Federal funds. Subgrantees of Federal funds submit cash advance requests through the CARDS cash advance module and report cash disbursements (expenditures) through the CARDS expenditure module to the Department. CARDS was implemented in July 2008, beginning with the cash advance module. In July 2009, the expenditure module was added to CARDS.

FINDINGS AND RECOMMENDATIONS

Cash Management

Finding No. 1: Cash Management Controls Over Federal Awards

Title 34, Section 80.20, Code of Federal Regulations (CFR), provides that grantees must establish reasonable procedures to ensure the receipt of reports on subgrantees' cash balances and cash disbursements in sufficient time to enable the preparation of complete and accurate cash transaction reports. This Section also provides that procedures for minimizing the time between the transfer of funds from the United States (U. S.) Treasury and disbursement by grantees and subgrantees must be followed whenever advance payment procedures are used. Additionally, Title 34, Section 80.21, CFR, provides that grantees and subgrantees shall promptly, but at least quarterly, remit interest earned on advances to the Federal agency except that the grantee or subgrantee may keep interest amounts up to $100 per year for administrative expenses. On June 15, 2010, the Department received a memorandum from the U. S. Department of Education reminding grantees of existing grant management requirements regarding payments, including, in part, requirements that grantees must regularly monitor the payment requests made by their subgrantees to ensure that the requests conform to the same payment requirements that apply to the grantee, regularly monitor the fiscal activity of the subgrantees on a continuous basis, and ensure that their subgrantees return interest earned. Furthermore, the Department's *Project Application and Amendment Procedures for Federal and State Programs Green Book*, Section C – Fiscal and Program Accountability, states that in accordance with Federal regulations, cash should be requested no more than three business days from the anticipated date of disbursement.

The Department provided advance payments to subgrantees to fund Federal awards expenditures. The Department established CARDS to provide users with information on the financial status of Federal awards projects. The subgrantees used CARDS to request cash advances and report cash disbursements. During the 2010-11 fiscal year, cash advances totaling $3,924,594,328 and disbursements totaling $3,893,287,811 were recorded in CARDS. Subgrantees could enter cash advance requests into CARDS throughout the month for any amount up to the amount of the project allocation less previous cash advances. Cash advance processing occurred once daily. Cash disbursement transaction processing took place on the 20th of each month. The Department required the subgrantees to enter cash disbursement transactions into CARDS by the 20th of the month following the month of disbursement. The Department did not have written procedures for the Federally required monitoring to ensure that the subgrantees adhered to the Federal payment and remittance of interest requirements. Additionally, Department management could not provide documentation to demonstrate that the Federally required monitoring of subgrantees' payment requests and fiscal activity, including subgrantee cash on hand, had occurred.

Department management stated, in response to audit inquiry, that the Department monitors cash by the subgrantees through the review of Auditor General audit reports and through CARDS. However, the Department cannot effectively monitor based on postaudits completed after the period is over. Regular monitoring on a continuous basis normally includes activities occurring throughout the award period to ensure the timely detection of subgrantee noncompliance with cash management requirements for Federal funds, should it occur.

The U. S. Treasury incurs additional borrowing costs when the Department draws and disburses Federal funds to subgrantees in advance of their immediate cash needs. The U. S. Treasury must borrow the cash needed to fund Federal programs and, as a result, incurs interest costs. Federal program funds drawn too early by a grantee results in additional Federal borrowing costs that would not have been incurred had the grantee not disbursed funds to the

subgrantees so far in advance of the subgrantees' immediate cash needs. Failure by the Department to monitor subgrantees' cash on hand and failure to ensure that the subgrantees properly calculate and remit any applicable interest earned on Federal cash advances, increases the risk of noncompliance with Federal regulations. This could result in Federal disciplinary action against the grantee, such as placement on a cash-reimbursement payment method, designation as a high-risk recipient, denial of funding, debarment or suspension, or other corrective actions including termination of awards.

Recommendation: The Department should establish written procedures to monitor its subgrantee payment requests and fiscal activity pursuant to Federal requirements, including, in part, procedures to proactively monitor subgrantee cash on hand prior to approving cash advances and monitoring procedures to ensure that subrecipients properly calculate and remit interest earned on Federal cash advances, when applicable.

Security Controls

Finding No. 2: Appropriateness of Access Privileges

Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction. As previously discussed, CARDS provides information on the financial status of Federal awards projects. Our audit test of the appropriateness of access to the CARDS production database, the CARDS database and application servers, CARDS programs, and the CARDS application disclosed that some employees and contractors had inappropriate or unnecessary access privileges, including unrestricted or elevated access to CARDS data and application programs, that increased the risk of unauthorized disclosure, modification, or destruction of CARDS data and application programs, as described in the following paragraphs.

Two employees with CARDS application programming duties had access to the CARDS production database through a fixed database role that allowed the employees to perform any activity in the database including grant and revoke access; create tables, stored procedures, and views; run backups; schedule jobs; modify or delete data; and add or delete databases. The same two employees could also create views and procedures through a user-defined database role. This level of access to the database was not appropriate for application programmers. These two employees also had administrator-level access to CARDS. This level of access within the application provided unrestricted user update capabilities and was contrary to an appropriate separation of programming and application end-user duties.

Seven employees within the Comptroller's Office, eight employees and contractors within Internal Applications Support, and the CIO were mistakenly granted a user-defined database role that had elevated permissions in the database. These employees and contractors were added to a security group that was intended to only have read permissions. However, this security group had previously been assigned the role with elevated permissions. Although CARDS restricted what these employees and contractors could access through the application, with the database role the employees and contractors could gain access to certain CARDS data through the database, external to CARDS application controls, that allowed execution of stored procedures that would update or delete data.

One database administrator and two database analysts shared common local user accounts in the Administrators group on the CARDS database server and application server. The use of shared user accounts may limit management's ability to establish responsibility for specific activities performed on the servers.

A local user account for one employee in the Comptroller's Office who performed programming duties on the CARDS application was included in the Administrators group on the CARDS application server. Being in the

Administrators group on the application server provided the employee complete control of the server (similar to a systems administrator), which provided the capability to install or delete software; configure the operating system; add or delete user accounts; modify security policies; and add, modify, or remove critical system files. This employee was one of the two employees described above who had unrestricted access to the CARDS production database and application.

Three contractors had local user accounts in the Administrators group on the CARDS application server. Two of the contractors no longer required this level of access for their job duties. The third contractor, who also had a domain user account, terminated contractual services in January 2010. Upon termination of the contract, the domain user account was disabled but, as of August 3, 2011, the local user account on the server had remained active for 569 days beyond termination. As discussed above, being in the Administrators group on the server provided the user complete control of the server. Retaining the local user accounts on the CARDS application server increased the risk that the elevated access privileges associated with the accounts may be misused by current and former contractors or others.

Effective controls over the modification of application programs help ensure that only authorized programs and authorized modifications are implemented. Source programs (the code created by application programmers) are compiled into object (executable) programs that are machine readable and used during data processing. To ensure an appropriate separation of duties, it is essential to adequately restrict and separate access to source program code, access to executable program code, and access to move programs into the production environment. A Department employee and a contractor had combinations of access privileges that were contrary to an appropriate separation of program change duties and could render application change management controls ineffective because the excessive access capabilities could allow for unauthorized changes to be made to the application programs and then concealed to prevent detection. Specifically:

- The employee with programming responsibilities described above, who had unrestricted access to the CARDS production database, application, and application server, also had elevated access capabilities on the change control database and in the change control application.
- A contractor, who no longer required access for his job duties, had unrestricted access to the change control server and, as discussed above, the CARDS application server, providing complete control over all IT resources on both servers. These combinations of access privileges provided the capability for one person to make program changes to CARDS application programs and implement the changed programs in the production environment.

Recommendation: The Department should remove the inappropriate access privileges to the CARDS production database, the CARDS database and application servers, the change control database and application, and CARDS. The Department should also evaluate employee and contractor job duties relating to CARDS and make changes to establish an appropriate separation of incompatible duties such as systems administration, database administration, application programming, user acceptance testing, movement of programs to production, and application data updates. Additionally, the Department should establish individual user accounts for the database administrator and analysts to ensure individual accountability and ensure that access privileges to IT resources are disabled in a timely manner when the user no longer requires the access privilege.

Finding No. 3: Timely Disabling of CARDS Access Privileges

Effective IT access controls include provisions for timely disabling of employee access privileges when employment terminations occur. Prompt action is necessary to ensure that the former employee or others do not misuse the former employee's access privileges.

Access privileges to CARDS are granted through the assignment of CARDS user logins. We tested 46 CARDS user logins assigned to Department employees as of February 11, 2011, to determine if any logins belonged to former employees. We compared all 46 user logins to an employee terminations list for the period July 2010 through February 2011 and found that seven former employees had been given CARDS access. Of the seven former employees, two did not have their CARDS access disabled in a timely manner. Specifically, the two former employees retained access privileges to CARDS for 8 and 114 days beyond their termination dates. The access privileges of the two former employees were not used subsequent to the dates of their employment termination. Nevertheless, without the timely disabling of former employee access privileges to CARDS, the risk was increased that the access privileges may be misused by the former employee or others.

Recommendation: The Department should ensure that the CARDS access privileges of former employees are timely disabled to minimize the risk of compromising CARDS data and IT resources.

Finding No. 4: CARDS Access Authorization Documentation

Effective security controls include logical (electronic) access controls that restrict legitimate and appropriate users to the specific IT resources needed and prevent others from accessing the resources. Access controls include, among other things, the use of access authorization forms to document the access privileges that have been authorized by management to be granted to system users.

According to Department procedures, a potential user must complete an access authorization form to obtain access privileges to CARDS. Our review of access authorization forms for a sample of ten Department employees with CARDS access disclosed that nine forms included in our sample were not reflective of the actual CARDS access privileges that had been granted to the employees. The access privileges for eight of the nine employees did not appear to be excessive. However, one employee's access privileges exceeded what was necessary for his job duties, as previously discussed in Finding No. 2. The discrepancies between the access authorization forms and access privileges that had been granted may limit management's ability to monitor the appropriateness of CARDS access privileges.

Additionally, one form included in our sample lacked the approval signature of the employee's supervisor. Consequently, it was unclear from Department records whether the employee's supervisor had authorized the access privileges that had been granted to the employee.

Recommendation: The Department should ensure that management appropriately documents authorization of all CARDS access privileges and that granted access privileges are reflective of what management has authorized.

Finding No. 5: Access Control Records Retention

The State of Florida, *General Records Schedule GS1-SL for State and Local Government Agencies (General Records Schedule)*, revised by the Department of State effective August 2010, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment.

The Department did not retain complete access control records for users with access privileges to CARDS, contrary to the requirements of the *General Records Schedule*. Access records for CARDS contained only the latest status of the CARDS user account and did not maintain a history record of each time the user account status changed. Without

the adequate retention of access control records, the risk was increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur. Additionally, the Department is not in compliance with the State's record retention requirements.

Recommendation: The Department should retain complete access control records pursuant to the *General Records Schedule* requirements.

Finding No. 6: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to user authentication that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls related to user authentication, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should implement appropriate security controls related to user authentication to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit during the period January 2011 through June 2011 and performed selected audit procedures through August 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to CARDS in achieving management's control objectives in in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, and reliability of data; and the safeguarding of IT resources.

The scope of our audit focused on evaluating selected IT controls applicable to CARDS. The audit included selected general IT controls over logical access to programs and data and application change management. The audit also included data exchange controls between CARDS and other significant systems and other selected CARDS application IT controls and selected user controls relevant to CARDS. Our audit included examinations of various Department records and transactions (as well as events and conditions) occurring from July 2010 through June 2011 and selected Department actions through August 2011.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of CARDS; including the purpose of the application and identification of the users; network structure, processing location, hardware, software, and user environments; the application data flow and interfaces with the Grants Management System and Florida Accounting Information Resource Subsystem (FLAIR) and applicable manual reconciliation procedures; access authorization process for CARDS and system resources; and the application change management process.
- Tested the appropriateness of selected CARDS input, processing, and output control procedures related to cash advances requested in CARDS.
- Evaluated the adequacy of monitoring for completeness and accuracy of awards transmitted from the Grants Management System to CARDS.
- Evaluated the effectiveness of exception reports and manual follow-up activities related to CARDS processing of cash advance and expenditure transactions.
- Evaluated, on a sample basis, the effectiveness of data exchange controls between CARDS, the Grants Management System, and FLAIR. Specifically, we reviewed a sample of three of four key interface points between the systems to determine if controls were in place to ensure that the data exchanges were complete and that the receiving systems acknowledged receipt of the data.
- Tested the appropriateness of user access privileges granted to CARDS for Department employees.
- Tested the appropriateness of logical access privileges to system resources (network, host operating system, database), including administrator access, related to CARDS. Specifically, we evaluated the appropriateness of access privileges granted to the CARDS production database and the appropriateness of elevated access privileges granted to the CARDS database server and the CARDS application server.
- Tested the appropriateness of logical access privileges to CARDS programs. Specifically, we evaluated the appropriateness of access privileges granted to the program change control application, the change control database where CARDS source program code resided, the change control server where the change control application and database resided, and the application server where the CARDS executable programs resided.
- Evaluated, on a sample basis, the effectiveness of procedures for authorizing user access privileges to CARDS for Department employees. Specifically, we reviewed a sample of 10 of 38 Department employee CARDS user accounts to determine whether the access authorization forms were on file and had appropriate supervisory signatures and whether the access privileges authorized on the forms were reflective of the actual access privileges granted.
- Tested the effectiveness of disabling CARDS user access privileges for Department employees who had transferred or terminated employment.
- Tested the adequacy of the use of application password controls for CARDS. Specifically, we tested the password length and composition and password change interval parameters related to CARDS.
- Tested the adequacy of the password policy and the use of password controls for the IT resources related to CARDS. Specifically, we evaluated the adequacy of Department policies and system-enforced requirements (settings) for password length and composition, password change interval, password prohibited reuse (enforce password history), password lockout, and password encryption within the CARDS application and database servers, CARDS database, change control server for CARDS, and the network domain.
- Evaluated the appropriateness of CARDS project cash advances that exceeded the project allocations.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

- We did not test the effectiveness of CARDS application change management controls such as controls to ensure that CARDS application changes were appropriately authorized, documented, tested, approved for production, and moved into production because of the excessive access capabilities and lack of an appropriate separation of incompatible duties with regard to CARDS data and application programs that were disclosed in other audit tests and described above in Finding No. 2.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated October 25, 2011, the Commissioner of Education provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

FLORIDA DEPARTMENT OF EDUCATION

STATE BOARD OF EDUCATION

KATHLEEN SHANAHAN, Chair
ROBERTO MARTÍNEZ, *Vice Chair*

Members
SALLY BRADSHAW
GARY CHARTRAND
DR. AKSHAY DESAI
BARBARA S. FEINGOLD
JOHN R. PADGET

Gerard Robinson
Commissioner of Education

Just Read, Florida!

October 25, 2011

David W. Martin, CPA
Auditor General
111 West Madison Street
G74 Claude Pepper Building
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Please find attached the Department's response to the Auditor General audit of the *Information Technology Operational Audit of the Department of Education, Cash Advance and Reporting of Disbursements System (CARDS).*

If you have any questions, please contact Peter Williams, Inspector General at (850) 245-0403 or Greg White, Director of Audits, Inspector General Office at (850) 245-9416.

Sincerely,

Gerard Robinson

GR/pw/dm

Enclosure

c: Ms. Linda Champion, Deputy Commissioner
Mr. Jon Manalo, Comptroller
Mr. Peter Williams, Inspector General
Mr. David Stokes, Chief Information Officer
Ms. Martha Asbury, Assistant Deputy Commissioner
Mr. Jon Ingram, Audit Manager, Auditor General Office

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

I. CASH MANAGEMENT

Finding No. 1: The Department did not have written procedures and had not implemented processes for monitoring subgrantee cash on hand from federal cash advances and for subgrantee calculation and remittance of interest earned on cash advances.

Response No. 1: The Department does monitor cash requests by the subgrantees through review of the Auditor General's audit reports and through the Cash Advance and Reporting of Disbursements System (CARDS) to ensure that requests are reasonable. The Department will document these existing processes. Since the inception of CARDS, only three audit findings related to districts' cash management or federal interest remittance have been received. This fact indicates that districts are appropriately identifying the specific federal programs prior to requesting advances for their cash needs. Furthermore, the recent monitoring visit by the U.S. Department of Education on the State Fiscal Stabilization Funds revealed no issues with the Department's monitoring processes on subgrantee's cash management or remittance of interest earned. The Department believes these processes are appropriate and that they meet the requirements. However, since the Department does require the subgrantees to report expenditures on a monthly basis, the Department will compare expenditures with the cash disbursed to identify the subgrantee's cash position to further strengthen the monitoring process.

II. SECURITY CONTROLS

Finding No. 2: The access privileges of some employees and contractors to CARDS and related IT resources were not appropriate for their job responsibilities and did not enforce an appropriate separation of incompatible duties.

Response No. 2: Reduced staffing resources limit the ability to achieve complete separation of duties. However, procedures to review access privileges have been developed and are being implemented to ensure that inappropriate access privileges are addressed. The Department will mitigate this issue through Change Management processes and Emergency Change Management processes as outlined in internal operating policies that have been developed for executive management approval. Additionally, audit logs will be used to track changes and activity by appropriate staff. Shared common accounts will no longer be allowed. Each user will authenticate with an individual account. Accounts will be reviewed on a regular basis to ensure inactive accounts are disabled in a timely manner.

Finding No. 3: The Department did not timely disable the CARDS access privileges of two former employees.

Response No. 3: At the time of the audit, the Department was implementing a process to ensure that access privileges of former employees were disabled in a timely manner. Reorganization of staff resources to accomplish this, as well as additional documentation of procedures, was finalized by the end of the audit.

Finding No. 4: The Department's CARDS access authorization forms were not reflective of the actual CARDS access privileges that had been granted to some employees. Additionally, the access authorization form for one Department employee included in our sample lacked the approval signature of the employee's supervisor.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Response No. 4: As previously discussed in Response No. 3, procedures for access authorization were addressed during the time of the audit. The Department had already resolved this issue by the end of the audit.

Finding No. 5: Contrary to the requirements of the State of Florida, *General Records Schedule,* for the retention of access control records, the Department did not retain complete access control records for CARDS.

Response No. 5: A manual tracking process was developed in June 2011 to ensure appropriate records retention to comply with the State of Florida's *General Records Schedule*. The Department will investigate the potential for modifications to the existing database in order to maintain this history electronically.

Finding No. 6: Certain security controls related to user authentication needed improvement.

Response No. 6: Prior to the audit, the Department's Password Policy was submitted and is currently under review for formal adoption by the Department's Executive Management. The proposed policy addresses the auditor's findings related to authentication controls. The proposed Application Development Security Standards and Guidelines (a counterpart document to the proposed Information Systems Development Methodology) addresses security requirements in application development.