MEMORANDUM

TO : Donald Rappaport
Chief Financial and Chief Information Officer

FROM : Jim Cornell
Area Manager
Washington Field Office

SUBJECT: Final Audit Report: Review of GAPS Security (ACN: A1180013)

This is our subject audit report covering the results of our security assessment of the Departments Grant Administration and Payment System (GAPS). The objective of the review was to evaluate the security posture of the GAPS automated payment processes, including the production environment and associated information technology considerations within the Departments communication infrastructure.

The assessment identified a number of technical or procedural security exposures which affect the overall security surrounding the GAPS production environment. They are directed to you for your action as either the Chief Financial Officer or the Chief Information Officer. To assist you in your determination of the relative significance of the review observations, we have categorized them as to high, moderate or low risk. Many of the exposures were discussed with the Office of Chief Financial Officer (OCFO) officials and Department of Education Central Automated Processing System (EDCAPS) contractor staff during the course of the review. Due to the sensitivity of the exposures and recommendations identified during the review, we are not including detailed information in this report. That information will be provided to you under separate cover.

Summary Findings

The review of GAPS security identified a number of opportunities for the enhancement of the overall security posture of the production application and its operational platform. Improvements can be made in the areas of security access control, security

option settings, audit trail controls, cash management, security administration, ensuring accountability, and appropriate segregation of developers from security and application functions.

Security Option Settings. The router and computer systems used for the web server, and production GAPS database appeared to utilize an excessive number of default settings. Use of default settings without appropriate tailoring of the settings to the GAPS environment could allow individuals inadvertent unauthorized access to GAPS data and GAPS processes. In addition, other settings could be strengthened to make the security posture stronger.

Audit Trail Controls. During our review we noted several opportunities for the GAPS development team to enhance the use of audit trails and to limit the use of group user IDs. Audit trail controls are the primary detective controls used to evidence a series of events or transactions within an application. The use of group user IDs can significantly reduce the effectiveness of controls over user authentication and identification. Stronger audit trail controls should be implemented to protect the integrity of the information processed through GAPS. In addition, the access level of individual user IDs should be consistent with business requirements due to the sensitive nature of the application.

Cash Management Controls. Our review found weaknesses in the procedures with regard to certification of the use of Federal funds drawn through GAPS. A combination of preventive and detective controls are necessary to ensure adequate cash management of Federal funds. The use of a robust electronic signature-based process or an interim manual signature procedure can provide the Department with increased grantee accountability for Federal funding requests.

Security Administration. Our review identified a significant number of users that had been assigned to more than one user group, which may have permitted excessive and/or incompatible access levels to GAPS functionality. Assignment of new user groups responsibilities should be documented in a thorough manner to substantiate the business need for the additional user group. In addition, more specific procedures should be introduced to ensure individual users do not belong to more than one user group, or if necessary, documented as to the business reason of why the user requires additional access and how this additional access will be monitored.

General Security. Opportunities are present to improve general security controls over the application and operational platform.

For example, limiting of access to GAPS user documentation and processes to only those Internet users who are GAPS users; enforcement of mandatory password changes for GAPS user IDs; and automated techniques for ensuring external GAPS users are, in fact, the users they represent themselves to be for accessing GAPS, are the types of security improvements which can be made related to the GAPS application. In addition, our review also noted a significant number of ports within the communication infrastructure configured with modem devices, presenting Aback door@ opportunities into the Department=s network environment, including GAPS. Uncontrolled use of modems within the Department=s communication infrastructure limits the effectiveness of protection provided by its firewalls and routers.

Segregation of Duties. Our review identified several areas where controls can be strengthened to ensure adequate separation of duties within critical application functions. Super-users, developers, and managers are key individuals whose access should be limited to affect an appropriate segregation of duties which ensures compliance with OMB A-130, OMB A-127, and OMB A-123. Our review identified what appeared to be an inordinate number of super-user IDs and group IDs, given the nature of GAPS functionality. Though privileged user IDs of these types provide easy system access to troubleshooting the GAPS production environment, they also limit the ability for system managers to clearly identify and authenticate users with privileged access.

What We Recommend. We recommend that the OCFO take steps to improve the overall security posture of the GAPS application and related communication infrastructure by taking appropriate action on the specific recommendations related to the high and moderate risk observations included as an attachment to this report. Determination of the appropriate action should include consideration of the costs versus benefits, relative risk and any compensating controls impacting each audit observation. We also recommend that the low risk observations be given appropriate attention in the OCFO=s overall security strategy.

Background

The Department is upgrading and streamlining its core management work processes. This effort is known as EDCAPS. EDCAPS comprises a suite of software packages, both off-the-shelf and custom developed. It consists of the Financial Management System Software (FMSS), the Contracts and Purchasing Support System (CPSS), GAPS, and the Recipient System (RS).

The GAPS production application is a client-server system that includes both custom developed and commercial-off-the-shelf (COTS) software. GAPS makes use of Saros products, Plexus Flo Ware (workflow system), Watermark (imaging), PowerBuilder (development), and Cognos Impromptu (reporting). The various software components in GAPS reside on servers and on client workstations located within the ED Network (EDNET). This review did not extend to reviewing the security posture of Powerbuilder, Saros, or Cognos Impromptu.

Objective, Scope, and Methodology

The objective of our audit was to evaluate the security posture of the GAPS automated payment processes. It did not include an assessment of other components of EDCAPS, specifically, FMSS, CPSS, and RS. The review addressed the primary GAPS application and associated servers; components that provide communication pathways; and servers providing auxiliary processing. We conducted our fieldwork from June 1998 through August 1998, in accordance with government auditing standards. The scope of the review consisted of an assessment of 1) Infrastructure (Communications) Security, 2) Computer Security, 3) Application Security, and 4) Operations Security. To identify security controls relevant to the GAPS application, we interviewed responsible officials and operational staff from the Department's EDCAPS-GAPS development team. We tested controls and security features by interogating the communication infrastructure and production environment using proprietary script utilities.

Statement on Management Controls

As part of our review, we assessed the system of management controls, policies, procedures, and practices applicable to the automated GAPS payment processes. Our assessment was performed to determine the security posture of GAPS. For the purpose of this report, we limited our review to the assessment of the significant controls over the automated grant payment functions. Because of inherent limitations, a study and evaluation made for the limited purpose described above would not necessarily disclose all material weaknesses in the controls. However, our assessment identified methods to improve the security posture of the GAPS application. We have recommended improvements to the controls by implementing stronger security controls (both preventive and detective). These weaknesses and their effects are fully described as an attachment to this report.

Auditee Comments

We provided the OCFO officials and the EDCAPS contractor staff with preliminary findings and recommendations based upon the results of our review at the end our fieldwork. They were in general agreement with the intent of the recommendations and plan to take appropriate corrective action to mitigate the exposures. In addition, they expressed a strong interest toward working closely with our review team to reach a mutually agreeable resolution to correcting the underlying exposures.

Please provide us with your final response to each open high and moderate risk recommendation within 60 days of the date of this report indicating what corrective actions you have taken or plan, and related milestones. The low risk observations are included as other matters for your consideration, but do not require a response.

In accordance with Office of Management and Budget Circular A-50, we will keep this audit report on the OIG list of unresolved audits until all open high and moderate issues have been resolved. Any reports unresolved after 180 days from date of issuance will be shown as overdue in the OIG=s Semiannual Report to Congress.

Please provide the Office of Chief Financial and Chief Information Officer / Financial Services Post Audit Group and the Office of Inspector General / Planning, Analysis and Management Services Staff with semiannual status reports on corrective actions until all such actions have been completed or continued follow-up is unnecessary.

In accordance with the Freedom of Information Act (Public Law 90-23), reports issued by the Office of Inspector General are available, if requested, to members of the press and the general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation shown us by the EDCAPS project staff during this review. Should you have any questions concerning this review, please feel free to contact me on (202) 205-9538 or Brett Baker of my staff on (202) 205-9744.

cc: Paul Gilbreath