

March 26, 2002

CHARLES E. BRAVO
SENIOR VICE PRESIDENT, CHIEF TECHNOLOGY OFFICER

ROBERT L. OTTO
VICE PRESIDENT, INFORMATION TECHNOLOGY

SUBJECT: Audit Report - eServices Registration Application Development Review
(Report Number EM-AR-02-004)

This report presents the results of our audit of the eServices Registration Application Development (Project Number 01BS009IS000). This audit was a self-initiated review that was included in our fiscal year 2002 Audit Workload Plan.

The audit disclosed Postal Service program management did not: (1) follow an established systems development life cycle methodology during testing, (2) produce key deliverables, and (3) always include key security features during systems development. As a result, the Postal Service assumed an unnecessarily high risk that the application would not be developed according to requirements, and the information security requirements would not be independently validated and tested. Management has terminated the eServices Registration application and plans to incorporate many of the recommendations into the new integrated systems methodology being used to modify the eCapabilities registration application. Management's comments were responsive to our findings and recommendations. We recommend closure of all recommendations. Management's comments and our evaluation of these comments are included in the report.

We appreciate the cooperation and courtesies provided by your staff during the review. If you have any questions or need additional information, please contact Robert Batta, director, Electronic Commerce and Marketing, at (703) 248-2100, or me at (703) 248-2300.

Ronald D. Merryman
Acting Assistant Inspector General
for eBusiness

Attachment

cc: James W. Buie
Wayne H. Orbke
James L. Golden
Susan M. Duchek

TABLE OF CONTENTS

Executive Summary	i
Part I	
Introduction	1
Background	1
Objectives, Scope, and Methodology	2
Prior Audit Coverage	2
Part II	
Audit Results	4
Systems Development Life Cycle Methodology Not Followed During System Testing	4
No Testing of Critical Security Features	4
Recommendations	5
Management's Comments	5
Evaluation of Management's Comments	5
End User Requirements Were Not Always Incorporated	5
Recommendation	6
Management's Comments	6
Evaluation of Management's Comments	6
Unit Test Results Were Not Formally Documented, Retained, or Approved	6
Recommendation	7
Management's Comments	7
Evaluation of Management's Comments	7
Software Quality Assurance Representative Not Assigned	8
Recommendation	8
Management's Comments	8
Evaluation of Management's Comments	8
Key Deliverables Not Always Produced	9
Recommendation	10
Management's Comments	10
Evaluation of Management's Comments	10

Information Security Assurance Validation Not Accomplished	11
Recommendation	11
Management's Comments	11
Evaluation of Management's Comments	11
Other Observations	12
Recommendation	12
Management's Comments	13
Evaluation of Management's Comments	13
Appendix A. Glossary	14
Appendix B. Management's Comments	16

EXECUTIVE SUMMARY

Introduction

There are five major stages in the systems development life cycle. Each stage has several process points that need to be accomplished to develop a successful project. This report presents our audit of the testing and information security process points of the eServices Registration application. This is the first report in a series of Office of Inspector General (OIG) self-initiated reviews of Postal Service initiatives in the early phases of development. By early involvement in the process, the OIG can make recommendations to resolve issues in the early stages of development prior to system implementation. Studies indicated that it is up to 100 times more costly to make changes after a system is placed into production.

Our objectives were to determine if Postal Service management followed: (1) sound systems development life cycle processes, (2) produced key deliverables as identified by Postal Service management and industry standards, and (3) considered appropriate application security features during the testing and information security process points of the development of eServices Registration application.

Results in Brief

Our review of the eServices Registration application found that Postal Service program management did not: (1) follow an established systems development life cycle¹ methodology during testing, (2) produce key deliverables, and (3) always include key security features during systems development.

These problems occurred because program management: (1) did not use existing industry best practices to meet the needs of rapid application development,² (2) attempted to meet an unrealistic system implementation date set by Postal Service management, and (3) did not map test plans to the system requirements document.

As a result, the Postal Service assumed an unnecessarily high risk that the application would not be developed

¹A systems development life cycle is a logical process by which systems analysts, software engineers, programmers, and end-users build information systems and computer applications to solve business problems and needs.

²Rapid Application Development is a system solution that allows system developers to quickly begin either with or without clearly specified client requirements, but with flexibility in addressing them in an atmosphere of partnership between the end-user and the developers.

according to requirements, and that the information security requirements would not be independently validated and tested.

During this audit, we briefed senior Postal Service officials on the issues in this report. Following the briefing, the planned October 2001 launch was suspended until deficiencies noted during the review are corrected.

**Summary of
Recommendations**

We recommended management evaluate the testing process in lieu of the Postal Service requirements, retest the system as necessary, and document the results. We also recommended the Postal Service complete key deliverables and conduct independent testing and validation during the information security process.

**Summary of
Management's
Comments**

Following an OIG briefing with senior Postal Service officials on the identified issues, the planned October 2001 launch date was suspended until deficiencies noted during the review were corrected. Subsequently, the Postal Service has conducted an assessment of the cost/development impacts on both eServices Registration application and the current eCapabilities registration application. Based on the evaluation, it was determined that the eServices Registration application would be terminated and that the eCapabilities registration application would be enhanced to meet business needs.

Based on this decision, management did not address the specific recommendations in this report. However, many of the recommendations are being incorporated in the new integrated systems methodology being used to modify the eCapabilities registration application. Management's comments, in their entirety, are included in Appendix B of this report.

**Overall Evaluation of
Management's
Comments**

Management's comments are responsive. Since the eServices Registration application has been terminated, we recommend closure of all recommendations. Programmatic recommendations will be captured in a capping report.

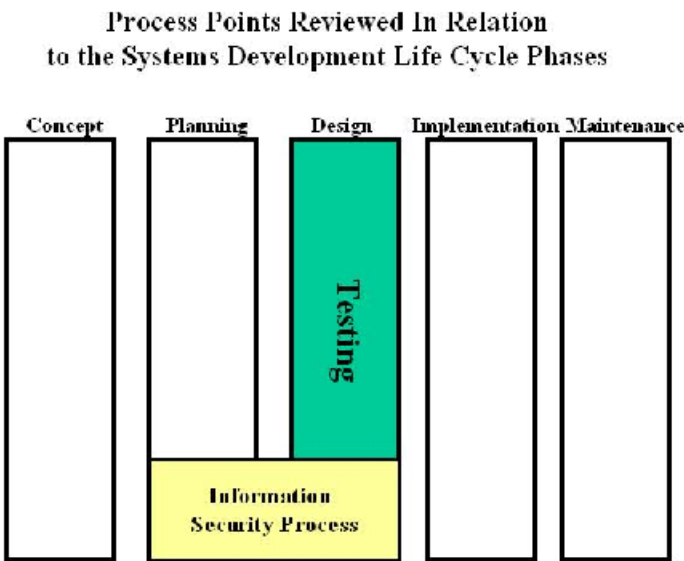
INTRODUCTION

Background

At the time of our audit, the Postal Service was developing the eServices Registration application to replace the eCapabilities registration and add login functionalities³ while providing additional features. The new application allows customers to sign on once to access numerous services, rather than signing on to each service.

The Postal Service created partnerships with other Internet organizations to create affiliate websites and developed websites to provide better customer service. In order to use the Postal Service web-based services or affiliate co-branded applications, users would be required to register through the eServices Registration application. The Postal Service planned that the eServices Registration application would support co-branded applications such as Amazing Mail, Net Post CardStore and Global Shipping Services. In addition, the eServices Registration application would support Postal Service web-based services such as USPS eBillPay, Mailing Online, NetPost Certified, and Customer Care.

Our review of the eServices Registration application occurred in the design phase during testing and evaluation. The chart below shows the two process points reviewed.



³Login functionalities provide a centralized platform for Postal Service customers to register for a wide variety of Postal Service services that have an Internet-based interface or capability (eServices).

During the testing process, the development team determines whether a software product meets its stated functional, technological, and security requirements. The information security process requires an independent team to validate that security policies have been incorporated into the system. Technical terms used in this report are described in Appendix A.

**Objectives, Scope,
and Methodology**

Our objectives were to determine if Postal Service management: (1) followed sound systems development life cycle processes, (2) produced key deliverables as identified by Postal Service management and industry standards, and (3) considered appropriate application security features during the testing and information security process points of the development of eServices Registration application.

To accomplish our objectives, we reviewed test plans, design and application requirement documents, and information security documents. We also reviewed test scripts to determine if testing of the eServices Registration application was meeting the applicable requirements.

We conducted audit fieldwork at Postal Service Headquarters and at the National Customer Support Center in Memphis, Tennessee, from September through October 2001. In addition, we reviewed applicable laws and regulations, as well as industry standards and industry best practices.⁴ This audit was conducted from September 2001 through March 2002 in accordance with generally accepted government auditing standards, and included such tests of internal controls as were considered necessary under the circumstances. We discussed our conclusions and observations with appropriate management officials and included their comments, where appropriate. We did not rely on computer generated data to accomplish our objectives.

Prior Audit Coverage

Our September 29, 2000, report, State of Computer Security in the Postal Service (Report Number IS-AR-00-004) cited that: (1) many Postal Service managers were not

⁴ We used Carnegie Mellon's Capability Maturity Model, Postal Service's Software Process Standards and Procedures, and Information System Audit and Control Association's Control Objectives for Information Technology.

fully aware of their responsibilities for computer security and, viewed computer security as the sole responsibility of the Information Technology office; (2) a lack of security awareness has resulted in less than sufficient emphasis placed on planning and budgeting for computer security; (3) policies and procedures for computer security were nonexistent, outdated, or oftentimes not implemented or followed; and (4) the National Information Systems Security organization did not have computer security enforcement authority, and was understaffed, underfunded, and not visible postal-wide. Management agreed with the Office of Inspector General's (OIG's) recommendations and indicated they are working to address the issues.

AUDIT RESULTS

Systems Development Life Cycle Methodology Not Followed During System Testing	<p>Program management did not follow an established systems development life cycle methodology during testing of the eServices Registration application. Specifically: (1) system testing did not include tests of all critical security features, (2) end users requirements were not always incorporated into customer acceptance testing, (3) test results were not formally documented, retained or approved, and (4) a software quality assurance representative was not assigned. As a result, program management could not ensure that the system met functional requirements or satisfy end user's requirements.</p> <p>Testing determines whether a software product meets its stated requirements. There are four levels of testing: (1) ?unit tests ensure each module works correctly; (2) ?integration tests examine the development of each subsystem; (3) ?system tests examine the entire system, including subsystem interfaces, system documentation, and overall functionality, to validate the design requirements have been met; and (4) customer acceptance testing, performed jointly with the end user, ensure that the system meets the end user's requirements.</p>
No Testing of Critical Security Features	<p>The program management team did not ensure that critical security features were tested. Specifically, cookies⁵ were not tested for known vulnerabilities such as corruption of data stored within cookies and viewing of cookies data by unauthorized personnel. In addition, intervals for refreshing the digital certificate⁶ key set were not established and tested. Further, security features such as audit trails, encryption, and Secure Socket Layer,⁷ while specified in the integration approach and software/hardware architecture documents, were not included in the testing requirements.</p> <p>Industry best practices recommend the testing of all programs, data, security functions/features, and technology requirements.</p>

⁵ A cookie generally is a short string of text that gathers information about the web user and his/her web-serving habits, and then returns this information back to the originating web-server.

⁶ A digital certificate is an electronic message that identifies the certificate authority, and the certificate owner, contains the owner's public key, identifies the certificate's operational period, contains a certificate serial number, and is digitally signed by the Certificate Authority.

⁷ Secure Socket Layer is industry standard technology used to protect web communications.

This occurred because program management did not map test plans to system requirements documents, Postal Service policies and procedures, and applicable laws to ensure all requirements were tested.

As a result, there is an increased risk the eServices Registration application would be implemented with serious security weaknesses. For example, cookies data may be corrupted or viewed by unauthorized personnel.

Recommendations	<p>We recommend the senior vice president, chief technology officer:</p> <ol style="list-style-type: none">1. Map existing test plans to system requirements documents, security requirements, as well as applicable sections of Section 508 of the Rehabilitation Act, Privacy Act of 1974, and Postal Service policies and procedures.2. Ensure test plans include tests of system requirements, perform tests, and take appropriate action(s) as required.
Management's Comments	<p>Management has terminated the eServices Registration application and plans to incorporate many of the recommendations in the new integrated systems methodology being used to modify the eCapabilities registration application. For that reason, management did not see any value in addressing specific recommendations contained in this report.</p>
Evaluation of Management's Comments	<p>Management's comments were responsive to our findings and recommendations. We recommend closure of these recommendations.</p>
End User Requirements Were Not Always Incorporated	<p>Program management did not incorporate several end user requirements into the customer acceptance testing efforts. Although many end user requirements were incorporated, we found instances where they were not incorporated. For example, an end user indicated the testing did not include the following requirements: (1) specific information for all NetPost Certified affiliated users, (2) population of edit fields for user address and organization information, and (3) capturing the user authorization identification.</p>

Industry best practices recommend that the development test team include end users in test reviews of system requirements and the final requirements document.

This occurred because the eServices Registration application development team had not incorporated all of the approved end user requirements at the time customer acceptance testing occurred. In addition, the development team did not involve end users in developing the customer acceptance testing test plan.

As a result, end users stated the system does not meet their business needs and may result in a loss of customer base and income. For example, the system does not populate edit fields with stored information on user address and organization information, but instead requires the end user to re-enter this information.

Recommendation	<p>We recommend the senior vice president, chief technology officer:</p> <ol style="list-style-type: none">3. Direct program management to incorporate end user requirements into the next release of the eServices Registration application requirements document and customer acceptance testing requirements, and involve end users in developing future customer acceptance tests.
Management's Comments	<p>Management has terminated the eServices Registration application and plans to incorporate many of the recommendations in the new integrated systems methodology being used to modify the eCapabilities registration application. For that reason, management did not see any value in addressing specific recommendations contained in this report.</p>
Evaluation of Management's Comments	<p>Management's comments were responsive to our finding and recommendation. We recommend closure of this recommendation.</p>
Unit Test Results Were Not Formally Documented, Retained, or Approved	<p>Program management did not ensure that test results were formally documented, retained or approved. Specifically, unit test results were not documented or retained. Further, unit and integration test results were not formally approved prior to moving the system to the next phase of testing.</p>

Industry best practices recommend that all unit test results should be documented in preparation for inspection, resolution of issues resulting from inspection, and baselining. In addition, industry best practices recommend that management define and implement procedures to ensure that operations and user management formally accepted the test results.

This occurred because program management had not followed industry best practices to ensure all test results were documented, retained or approved.

Therefore, the Postal Service has no assurance testing was accomplished and deficiencies noted during testing were corrected. Additionally, development team members were unable to benchmark new test results against old test results.

Recommendation

We recommend the senior vice president, chief technology officer:

4. Ensure test results are documented, retained, and approved prior to moving to the next phase of development. Once completed, retest, as appropriate.

**Management's
Comments**

Management has terminated the eServices Registration application and plans to incorporate many of the recommendations in the new integrated systems methodology being used to modify the eCapabilities registration application. For that reason, management did not see any value in addressing specific recommendations contained in this report.

**Evaluation of
Management's
Comments**

Management's comments were responsive to our finding and recommendation. We recommend closure of this recommendation.

Software Quality Assurance Representative Not Assigned	<p>Program management did not appoint an independent software quality assurance⁸ representative.</p> <p>Industry best practices states that at project initiation a software quality assurance representative should be appointed to independently facilitate the development, ensure all requirements are met, and deliver the system on time at the lowest possible cost.</p> <p>This occurred because program management did not follow existing industry best practice or establish an alternate system of controls.</p> <p>As a result, program management cannot ensure that the development process was appropriately monitored,</p> <p>established standards were followed, and system inadequacies were brought to management's attention.</p>
Recommendation	<p>We recommend the senior vice president, chief technology officer:</p> <p>5. Appoint an independent software quality assurance representative to the eServices Registration application project.</p>
Management's Comments	<p>Management has terminated the eServices Registration application and plans to incorporate many of the recommendations in the new integrated systems methodology being used to modify the eCapabilities registration application. For that reason, management did not see any value in addressing specific recommendations contained in this report.</p>
Evaluation of Management's Comments	<p>Management's comments were responsive to our finding and recommendation. We recommend closure of this recommendation.</p>

⁸ The Software Quality Assurance Representative independently facilitates the development of defect free products that meet all requirements and are delivered on time at the lowest possible cost.

**Key Deliverables Not
Always Produced**

Program management did not ensure key deliverables were produced, reviewed, and conducted before the planned system implementation. Specifically, they did not produce the operational readiness plan, deployment plan, performance test plan, data migration process plan, and business continuity and contingency plan.

Industry best practices recommend the project management team establish a project tracking schedule/reporting mechanism for development efforts. Further, it sets forth that comprehensive testing of systems must be performed to increase both the quality of systems delivered and the level of user satisfaction with those systems.

In addition, the information security policy states that business continuity and contingency planning is required for all information resources. The business continuity and contingency plan should provide cost effective recovery, protection of assets, and continuity of business operations.

This occurred because program management attempted to meet an unrealistic system implementation date set by Postal Service management. In addition, the development team had unexpected delays due to connectivity problems with other applications and contract coordination. Furthermore, the team anticipated using a contractor to develop a business continuity and contingency plan, however, they did not allocate time to put contractual documents in place.

As a result, there was an increased risk that the system would not be fully tested, properly deployed, and data would not be properly migrated during conversion. Furthermore, without a business continuity and contingency plan, the Postal Service may be unable to support the application in the event of a failure which may result in a loss of revenue and customer confidence.

Recommendation	<p>We recommend the senior vice president, chief technology officer:</p> <p>6. Complete the eServices Registration application operational readiness plan, deployment plan, performance test plan, data migration process plan, and a business continuity and contingency plan.</p>
Management's Comments	<p>Management has terminated the eServices Registration application and plans to incorporate many of the recommendations in the new integrated systems methodology being used to modify the eCapabilities registration application. For that reason, management did not see any value in addressing specific recommendations contained in this report.</p>
Evaluation of Management's Comments	<p>Management's comments were responsive to our finding and recommendation. We recommend closure of this recommendation.</p>

Information Security Assurance Validation Not Accomplished	<p>During the information security process, the independent validation of security requirements was not performed. Instead, the Certification and Accreditation teams relied on the project development team's assertions that security requirements were adequate, as well as results from OIG and other external reviews.</p> <p>Postal Service's AS-850-97-3, <u>Security Certification and Accreditation of Sensitive Applications and Systems</u> require the Certification team, lead by the Information Systems security officer, to review and validate the system security requirements.</p> <p>Security requirements were not validated because the Information Systems security officer did not believe the policy required an independent validation of security requirements. However, our review of the policy indicated that the Information Systems security officer's responsibilities include leading a review and validating security requirements.</p> <p>Independent validation is a critical control to safeguard the integrity, confidentiality, and availability of Postal Service information and to protect the interests of the Postal Service, its personnel, its business partners, and the general public.</p>
Recommendation	<p>We recommend the senior vice president, chief technology officer:</p> <p>7. Ensure independent testing and validation of security requirements are performed.</p>
Management's Comments	<p>Management has terminated the eServices Registration application and plans to incorporate many of the recommendations in the new integrated systems methodology being used to modify the eCapabilities registration application. For that reason, management did not see any value in addressing specific recommendations contained in this report.</p>
Evaluation of Management's Comments	<p>Management's comments were responsive to our finding and recommendation. We recommend closure of this recommendation.</p>

Other Observations

Although not part of the testing of information security processes, the eServices Registration application development team used software that had not been approved by the Infrastructure Tool Kit Requirement Committee.⁹ Specifically, during the development effort the team used web-based tools, such as IPlanet version 4.1 and Jrun. The IPlanet software is included in the current version of the approved Netscape Enterprise Server. However, no one could verify that all components of the IPlanet software were approved.

The Infrastructure Tool Kit provides guidelines on tools that support the development, deployment, and management of distributed applications. It includes a list of tools approved for use by Postal Service Information Technology, Architecture, and Engineering. When existing web-based tools change names or new versions are issued, the Infrastructure Tool Kit guidelines require the tool to go through the approval process.

This occurred because program management did not wait for approval of the web-based tools prior to use. The tools selected were common industry tools that program management had submitted to the Infrastructure Tool Kit Requirement Committee and expected to be approved.

As a result, the eServices Registration application development team utilized software products that may not receive continued support from the vendor. In addition, if the Infrastructure Tool Kit Requirement Committee does not approve the software, the eServices Registration application cannot be hosted or used on the Postal Service infrastructure and would have to be redeveloped.

Recommendation

We recommend the senior vice president, chief technology officer:

8. Ensure all software used in the development effort is approved by the Infrastructure Tool Kit Requirement Committee prior to use.

⁹ The Infrastructure Tool Kit Requirement Committee is composed of information technology and customer organization technical personnel.

Management's Comments	Management has terminated the eServices Registration application and plans to incorporate many of the recommendations in the new integrated systems methodology being used to modify the eCapabilities registration application. For that reason, management did not see any value in addressing specific recommendations contained in this report.
Evaluation of Management's Comments	Management's comments were responsive to our finding and recommendation. We recommend closure of this recommendation.

APPENDIX A. GLOSSARY

<u>Term</u>	<u>Description</u>
Accreditation	The official management authorization to operate a system
Business Continuity and Contingency Plan	Business continuity and contingency plan is a total management approach to providing cost-effective recovery, protection of assets, and continuity of business operations.
Certification	A process that develops a technical opinion and supporting documentation as to whether a system meets its security requirements.
Certification and Accreditation Team	The certification and accreditation team is responsible for working with the customer of the system and developers to ensure that certain basic security controls are incorporated into all sensitive systems during the design and development stages.
Cookie	A cookie generally is a short string of text that gathers information about the web user and his/her web-serving habits, and then returns this information back to the originating web-server.
Design and Application Requirements Document	The design and application requirements document is used to verify that requirements and design interfaces have been developed correctly.
Digital Certificate	A digital certificate is an electronic message that identifies the certificate authority, identifies the certificate owner, contains the owner's public key, identifies the certificate's operational period, contains a certificate serial number, and is digitally signed by the certificate authority.
Encryption	Encryption is the conversion of data into a form, called ciphertext that cannot be easily understood.
Information Systems Security Officer	Information Systems security officer performs the security certification process of the system and chairs the security certification committee.
Infrastructure Tool Kit Requirement Committee	The infrastructure tool kit requirement committee is composed of information technology and customer organization technical personnel.

APPENDIX A. GLOSSARY (Continued)

Login Functionalities	Login functionalities provide a centralized platform for Postal Service customers to register for a wide variety of Postal Service services that have an Internet-based interface or capability (eServices).
Rapid Application Development	Rapid application development is a system solution that allows system developers to quickly begin either with or without clearly specified client requirements, but with flexibility in addressing them in an atmosphere of partnership between the end user and the developers.
Secure Socket Layer	Secure socket layer is industry standard technology used to protect web communications.
Software Quality Assurance Representative	The software quality assurance representative independently facilitates the development of defect free products that meet all requirements and are delivered on time at the lowest possible cost.
Systems Development Life Cycle	A systems development life cycle is a logical process by which systems analysts, software engineers, programmers, and end users build information systems and computer applications to solve business problems and needs.
Test Plans	Test plans design and document a set of system tests to ensure that the application system delivered meets all of the requirements identified in the requirements document.
Unit Test	Testing determines whether a software product meets its stated requirements. Unit tests make sure each load module works correctly.

APPENDIX B. MANAGEMENT'S COMMENTS

ROBERT L. OTTO
VICE PRESIDENT - INFORMATION TECHNOLOGY



February 19, 2002

ROBERT L. EMMONS

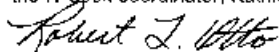
SUBJECT: Management Response to Draft Report for eServices Registration (eSR)
Application Development Review (Report Number EM-AR-02-DRAFT)

The Office of Inspector General's audit of eServices Registration application development review found that the Postal Service program management did not (1) follow an established systems development life cycle methodology during testing, (2) produce key deliverables, and (3) always include key security features during systems development. Following the briefing to senior Postal Service officials on the identified issues, the planned October 2001 launch date was suspended until deficiencies noted during the review were corrected.

Subsequently, the USPS.com Registration Steering Committee, comprised of representatives from the various business drivers, CTO and IT organizations, began to assess the need for an overall registration capability for USPS.com. The purpose was to determine the complete set of registration requirements from each organization, assess the cost/development impacts on both eSR and the current eCap registration systems, and select the system that would be used going forward. Based on the evaluation, including cost and a series of new registration requirements that were not part of the initial eSR or eCAP design, it was determined that eSR would be terminated and that the eCAP registration system would be enhanced to meet business needs.

Based on this decision we do not believe there is value in addressing the specific recommendations contained in the eSR audit report, however many of the recommendations are being incorporated in the new Integrated Systems Methodology initiative being driven by the VP, IT to provide overall system development processes and requirements.

If you have questions regarding our response and would like to discuss them further, please contact the IT audit coordinator, Kathleen Sober at (202) 268-6156.


Robert L. Otto

cc: John Edgar
James Golden
John Gunnels
Joyce Hansen