March 27, 2002

CHARLES E. BRAVO
SENIOR VICE PRESIDENT, CHIEF TECHNOLOGY OFFICER

ROBERT L. OTTO
VICE PRESIDENT, INFORMATION TECHNOLOGY

SUBJECT: Audit Report - Delivery Unit Notification System Application Development Review (Report Number EM-AR-02-006)

This report presents the results of our audit of the Delivery Unit Notification System 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 test critical security features. As a result, the Postal Service assumed an unnecessarily high risk that the Delivery Unit Notification System would not be developed according to requirements, and that the information security assurance requirements would not be independently validated and tested. Management agreed with our recommendations and has initiatives in progress, completed, or planned addressing the issues in this report. Management's comments and our evaluation of these comments are included in this 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 J. Batta, director, eCommerce 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

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 Delivery Unit Notification System. This is the second 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 audit objectives were to determine if the Postal Service: (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 the Delivery Unit Notification System.

Results in Brief

Our review of the Delivery Unit Notification System found that Postal Service program management did not: (1) follow an established systems development life cycle[1] methodology during testing, (2) produce key deliverables, and (3) always test critical security features.

These problems occurred because program management did not: (1) always follow existing Postal Service policies, procedures, and guidelines, (2) adequately define responsibilities of the development team members, and (3) designate members of the information security assurance team and provide necessary training on the new information security assurance process.

As a result, the Postal Service assumed an unnecessarily high risk that the Delivery Unit Notification System would not be developed according to requirements, and that the information security assurance requirements would not be independently validated and tested.

[1] 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.

Summary of Recommendations	The deployment of the Delivery Unit Notification System should be delayed until complete testing can be accomplished and desired results obtained. We recommended management prepare the business needs statement, business needs document, and finalize the requirements document. We also recommended before testing occurs, all requirements are addressed and traced to test scenarios and plans, and test constraints identified. Management should also designate and train members of the information security assurance team.
Summary of Management's Comments	Management agreed with our findings and recommendations. Corrective actions have been implemented for five of the twelve recommendations. Actions are under way to resolve the remaining items during fiscal year 2002. 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 to our findings and recommendations. We agree with the actions management has taken to date and the planned corrective action for each recommendation.

INTRODUCTION

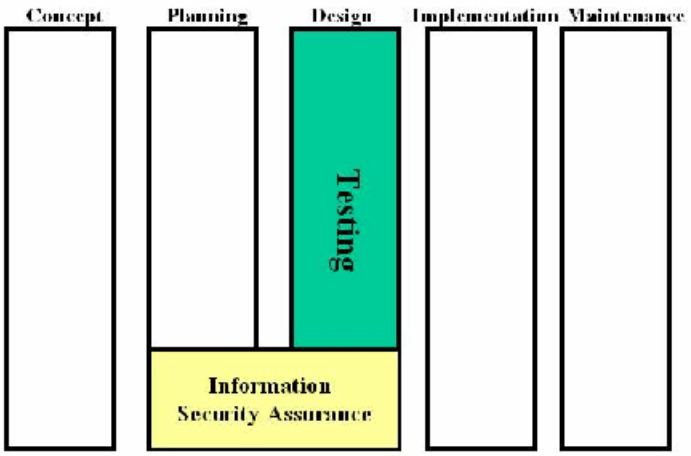
Background

The Postal Service is developing the Delivery Unit Notification System to enable customers to make hold mail and redelivery service(s) requests. In addition, the system will include a 360-degree feedback process to track performance and ensure service requests are fulfilled as required by the customers.

The Delivery Unit Notification System will use and build on the Call Center Management application, which already contains much of the infrastructure needed to support the system. The Call Center Management infrastructure is used by call center agents and responsible delivery units to handle three million hold mail and redelivery calls annually. A customer interface will be developed to capture customer requests for hold mail and redelivery service(s) and requests will be stored in the Call Center Management database.

We reviewed the design phase of the Delivery Unit Notification System during the testing and information security assurance processes. At the time of our review, the Delivery Unit Notification System was scheduled for implementation in November 2001.

Process Points Reviewed In Relation to the Systems Development Life Cycle Phases



During the testing process, the development team determines whether a software product meets its stated functional, technological, and security requirements. The information security assurance 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 audit objectives were to determine if the Postal Service: (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 the Delivery Unit Notification System.

Specifically, to accomplish these objectives, we reviewed test scripts and plans, design and application requirement documents, and information security assurance documents.

We conducted audit fieldwork at Postal Service Headquarters and at the Integrated Business Systems Solutions Center in Raleigh, North Carolina, from September 2001 through October 2001. In addition, we conducted interviews, and reviewed applicable laws and regulations, as well as industry standards and best practices.[2] This audit was conducted from September 2001 through March 2002, in accordance with generally accepted government auditing standards, and included 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 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

[2] Criteria cited in the report included Carnegie Mellon's Capability Maturity Model, Postal Service's Software Process Standards and Procedures, National Institute of Standards Special Publication 800-18, and Information System Audit and Control Association's Control Objectives for Information Technology.

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, under funded, and not visible postal-wide. Management agreed with Office of Inspector General's (OIG) recommendations and was working on corrective actions.

AUDIT RESULTS

Systems Development Life Cycle Methodology Not Always Followed During System Testing	Program management did not always follow an established systems development life cycle methodology during testing of the Delivery Unit Notification System. Specifically: (1) system testing did not include tests of all critical security features, (2) all end user requirements were not incorporated during the development effort, (3) test results were not always documented, retained or approved, (4) the test environment did not mirror the production environment, and (5) roles and responsibilities were not always assigned. As a result, program management could not ensure that the system met functional requirements or satisfied end users' requirements. Testing determines whether a software product meets its stated requirements. There are four levels of testing, unit tests ensure each module works correctly, ?integration tests examine the development of each subsystem, system tests examine the entire system, including subsystem interfaces, system documentation, and overall functionality, to validate the design requirements have been met. Customer acceptance testing performed jointly with the end user, ensure that the system meets the end user's requirements. We reviewed the Delivery Unit Notification System during the design phase testing and information security assurance processes. At the time of our review, the Delivery Unit Notification System was scheduled for implementation in November 2001. Corrective actions for the following recommendations should occur before the system is implemented.
Testing of Security Features Had Not Occurred	Program management did not test all critical security features. Specifically, security features such as audit trails, encryption, and Secure Socket Layer,[3] while specified in the integration approach and software/hardware architecture documents, were not included in the testing requirements. The Postal Service Software Process Standards and Procedures guideline recommended the testing of all program, data, security functions/features, and technology requirements. In addition, other Postal Service system development guidelines recommended that a master test

[3] Secure Socket Layer is industry standard technology used to protect web communications.

plan be developed. This plan would identify tests to be performed, test environment, hardware and software testing requirements, and test roles and responsibilities.

Testing of all critical security features did not occur because program management did not map existing test plans to the system requirements document, Postal Service policies and procedures, and applicable laws to ensure all requirements were tested. Further, the Postal Service had not developed a comprehensive testing approach that would have identified all tests to be performed.

As a result, there is an increased risk the Delivery Unit Notification System would be implemented with serious security weaknesses. For example, without proper encryption, unauthorized individuals may view Privacy Act protected information.

Recommendation	We recommend the senior vice president, chief technology officer: 1. Identify and list all critical security features by mapping existing test plans to system requirements documents, security requirements, as well as Section 508 of the Rehabilitation Act, Privacy Act of 1974, and Postal Service policies and procedures.
Management's Comments	Management agreed with our recommendation and will take corrective action by mapping existing test plans as recommended by April 5, 2002.
Recommendation	2. Develop a comprehensive testing approach that would include tests of all security features.
Management's Comments	Management agreed with our recommendation and will take corrective action by performing comprehensive testing for the Delivery Unit Notification System which will include testing of all security features. This will be completed by April 5, 2002.

Recommendation	We recommend the senior vice president, chief technology officer: 3. Modify test plans to include tests of all security features, perform these tests, and take appropriate action(s) as required.
Management's Comments	Management agreed with our recommendation and has taken corrective action by updating the security test plan to include tests for all security features. Management will take additional corrective action by resolving issues or problems identified in test results, and incorporate those results into the security plan and risk assessment documents by April 19, 2002.
Evaluation of Management's Comments	Management's actions taken to date and planned actions are responsive to recommendations 1 through 3.
Unit Test Results and Critical Requirements Were Not Always Documented, Retained, or Approved	Program management did not always ensure that test results were 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 into the next phase of testing. In addition, while the development team requested an approved business needs document, business needs statement and requirements document, these documents were in draft and had not been formally approved by the Integrated Business Systems Solution Center group, who had responsibility for developing the system. The Postal Service Software Process Standards and Procedures guideline recommend that unit test results should be documented in preparation for inspection, resolution of issues resulting from inspection, and base lining. In addition, industry best practices recommend that management define and implement procedures to ensure that operations and user management formally accepted the test results. Further, industry best practices recommend that business needs document, business needs statement, and the requirements document are formally approved by the developer, customer, and end user.

Test results were not always documented and approved because program management had not followed Postal Service guidelines and industry best practices prior to moving forward with the project.

Therefore, the Postal Service has no assurance testing was accomplished and that deficiencies noted during testing were corrected. Additionally, development team members were unable to benchmark new test results against old test results. Further, without an approved business needs statement, business needs document, and requirements document; the Postal Service cannot ensure the system will meet business needs.

Recommendation

We recommend the senior vice president, chief technology officer ensure:

4. Test results are documented, retained, and approved prior to moving into the next phase of development.

Management's Comments

Management agreed with the recommendation the Delivery Unit Notification System project followed Postal Service Software Process Standards and Procedures guidelines regarding documentation of test results. The results of unit and integration test completed as of the September 17, 2001, audit date were documented, retained and provided to the OIG on September 20, 2001. Additional testing including system, security, and Customer Acceptance Testing will be performed by April 25, 2002. These test results will be documented, retained, and approved prior to moving into the implementation phase.

Evaluation of Management's Comments

Management comments are responsive to the recommendation that the Software Process Standards and Procedures guidelines were followed for integration tests and these results were provided to the OIG. No unit test results were provided to the OIG during the audit fieldwork. Unit test results were provided to the OIG in March 2002. We agree with the subsequent corrective actions the Postal Service has taken to conduct additional testing and the plan to conduct, document, retain, and approve additional tests in this area.

Recommendation	We recommend the senior vice president, chief technology officer ensure: 5. The business needs statement, business needs document, and requirements document are approved and provided to the development team.
Management's Comments	Management agreed with our recommendation and took corrective action on September 21, 2001, by ensuring that the business needs statement, business needs document, and requirements document were signed off by the portfolio manager and later provided to the development team.
Evaluation of Management's Comments	In response to our audit, the development team did receive the proper documents and this action was responsive to our recommendation. At the time of our fieldwork the development team had not received copies of the signed business needs statement, business needs document, and requirements document. We recommend closure of this recommendation.
Test Environment Different From Production Environment	Delivery Unit Notification System program management did not ensure that the test environment mirrored the production environment. For example, hardware components were not in place for the testing environment to mirror the production environment. Based on industry best practices and National Institute of Standards and Technology Special Publication 800-18, hardware and software unit, string, and customer acceptance tests should be conducted in a test environment that matches the production environment. The test environment did not mirror the production environment[4] because Postal Service management had not provided funding for a production environment. Without a production environment, the development team could not define hardware and interface requirements for the system. As a result, the Postal Service had no assurance that the tested system will operate the same in the production environment.

[4] The production environment is the staging area or environment for the actual system operation.

Recommendation	We recommend the senior vice president, chief technology officer: 6. Define hardware and interface requirements for the Delivery Unit Notification System once a production environment has been established.
Management's Comments	Management agreed with our recommendation and took corrective action on January 29, 2002, by completing an architectural design document, which included hardware and software interface requirements.
Evaluation of Management's Comments	Management's actions taken are responsive to our recommendation. We recommend closure of this recommendation.
Recommendation	7. Perform system testing in an environment, which mirrors the production environment.
Management's Comments	Management agreed with our recommendation; however, due to a freeze on capital spending, they were unable to purchase hardware to replicate the production environment for testing. Hosting of the Delivery Unit Notification System will now be provided in-house and the Postal Service will temporarily assign hardware for testing purpose by April 12, 2002.
Evaluation of Management's Comments	Management's planned actions are responsive to our recommendation.
Independent Quality Assurance Representative Not Assigned	Program management did not appoint an independent software quality assurance representative[5] for the Delivery Unit Notification System development effort.

[5] 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.

The Postal Service Software Process Standards and Procedures guidelines recommend that at project initiation a software quality assurance representative should be appointed to each project.

A software quality assurance representative was not appointed because program management did not follow existing Postal Service guidelines.

As a result, program management cannot ensure that the development process was appropriately monitored, established standards were followed, and system inadequacies were brought to management's attention.

Recommendation	We recommend the senior vice president, chief technology officer: 8. Ensure a software quality assurance representative is appointed to the Delivery Unit Notification System project.
Management's Comments	Management agreed with our recommendation and took corrective action on December 14, 2001, by appointing and independent software quality assurance representative to the Delivery Unit Notification System.
Evaluation of Management's Comments	Management's actions taken are responsive to our recommendation. We recommend closure of this recommendation.

A Key Deliverable Was Not Produced	Program management did not ensure a key deliverable, that is a risk assessment, was produced and reviewed. The Software Process Standards and Procedures guideline state the project manager, with assistance from the business systems manager and project analyst, develop a risk assessment that identifies risks that may impact the cost, resources, schedule, and technical aspects of the project. The information security assurance process required the completion of a risk assessment for all sensitive, critical, or business-controlled information resources. The risk assessment identifies the assets at risk, weaknesses, vulnerabilities, and possible safeguards. Additional risks may be identified as development progresses through the various systems development life cycle stages. Program management did not perform a risk assessment because they believed that completion of the risk assessment requirement under the information security assurance process occurred after testing. However, the information security assurance process requires risk assessments to be performed as the project progresses through the systems development life cycle. Without a risk assessment, certain risks inherent in the system may be overlooked and compromised.
Recommendation	We recommend the senior vice president, chief technology officer: 9. Complete a risk assessment for the Delivery Unit Notification System project, which identifies risks that may impact the cost, resources, schedule, security, and technical aspects of the project.
Management's Comments	Management agreed with our recommendation and completed a security risk assessment for the Delivery Unit Notification System. In addition, the Postal Service will take corrective action by April 12, 2002, by documenting any remaining risks and properly managing and mitigating those risks following management guidelines.
Evaluation of Management's Comments	Management's planned and implemented actions are responsive to our recommendation.

Information Security Assurance Validation Not Accomplished

During the information security assurance process, the Information Systems security officer did not perform independent validation of security requirements.

The new information security assurance process replaced the prior security certification and accreditation review process. The process requires the Certification team prepare the information security assurance package that includes system documentation and test results. In addition, the information security assurance policy requires an independent team that includes the Information Systems security officer, to review the information security assurance package, perform independent validation of assertions, and independently test the system. Upon completion of the review, the Information Systems security officer reviews the information security assurance package, prepares an evaluation report, and forwards any findings to the accreditor.

Independent validation of security requirements was not performed because program management had not yet designated members of the information security assurance team and provided them with the necessary training on the new information security assurance process.

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, business partners, and the general public.

Recommendation

We recommend the senior vice president, chief technology officer:

10. Ensure independent testing and validation of security requirements are performed during the information security assurance process.

Management's Comments

Management agreed with our recommendation and will take corrective action by having an independent test group perform independent testing and validation of the security requirements by April 19, 2002.

Evaluation of Management's Comments	Management's planned actions are responsive to our recommendation.
Recommendation	We recommend the senior vice president, chief technology officer: 11. Designate information security assurance team members and provide them the necessary training.
Management's Comments	Management agreed with our recommendation and took corrective action on November 16, 2001, by designating an information security assurance team and having those members receive training.
Evaluation of Management's Comments	Management's actions taken are responsive to our recommendation. We recommend closure of this recommendation.

Other Observations

Although not part of the testing or information security assurance processes, the Delivery Unit Notification System development team used software that had not been approved by the Infrastructure Tool Kit Requirement Committee.[6] Specifically, the team used the web-based tools Netscape IPlanet, and Unibar.

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 the Postal Service information technology architecture and engineering group. All changes to existing web-based tools names or versions must be approved by the Infrastructure Tool Kit Requirement Committee.

Program management did not use approved software because it did not allow for approval of the web-based tools prior to use. The tools selected were common industry tools that program management expected to be approved.

As a result, the Delivery Unit Notification System development team utilized software products that may not receive continued support from the vendor. In addition, if the Infrastructure Tool Requirement Committee does not approve the software, the 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:

12. Ensure that all software used in the development effort is approved by the Infrastructure Tool Kit Requirements Committee prior to use.

Management's Comments

Management agreed with our recommendation and took corrective action on October 31, 2001, by having all software used in the development effort approved by the Infrastructure Tool Kit Requirements Committee.

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

Evaluation of Management's Comments	Management's actions taken are responsive to our recommendation. We recommend closure of this recommendation.

APPENDIX A. GLOSSARY

Term	Description
Business Needs Document	Business needs document is a joint client and developer activity. Users and clients define in nontechnical, business terms what is needed, how the new system is supposed to behave, and how existing manual and automated systems currently perform.
Business Needs Statement	Business needs statement is a brief statement prepared jointly by the Business Systems manager, client, and end-users to identify the high-level business needs that the system will satisfy.
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.
Design and Application Requirements Document	The design and application requirements document is used to verify that requirements and design interfaces have been developed correctly.
Encryption	Encryption is the conversion of data into a form, called ciphertext that cannot be easily understood.
Information Security Assurance Process	The information security assurance process is the Postal Service process for protecting the confidentiality, integrity, and availability of its information resources.
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.
Production Environment	The production environment is the staging area or environment for the actual system operation.
Risk Assessment	An analysis that examines an organization's information resources, its existing controls, and its remaining organization and computer system vulnerabilities.

APPENDIX A. GLOSSARY (CONTINUED)

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 Environment	Test environment is utilized by the analysts and programmers to develop and maintain programs.
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

Charles E. Bravo
Chief Technology Officer
Senior Vice President

UNITED STATES POSTAL SERVICE

February 19, 2002

MR. EMMONS

SUBJECT: Draft Interim Report for Delivery Unit Notification System (DUNS)) Application Development Review (Report Number EM-AR-02-DRAFT)

This provides the management response to the above referenced draft audit report. In addition to the attached corrective action plans, this response also contains comments and clarifications regarding the body of the audit report, which we believe should be incorporated into the final audit report to ensure the recommendations are interpreted in the proper context.

Findings

We agree there is value in the early identification of potential concerns, when the issues can be resolved in a cost effective manner. However, it is important to understand that the DUNS audit was conducted during the design phase; but prior to the completion of the testing and information security activities. For this reason, several of the deliverables and activities, which were recommended in the audit report, were planned but not yet scheduled to be completed.

Further, the audit report may give a misimpression that the development team did not follow an established System Development Lifecycle methodology during the testing phase. The audit report should reflect that the postal service Software Process Standards and Procedures (SPSP) guidelines were followed and only certain aspects of the DUNS deliverables require further effort.

Corrective actions have been implemented for five (5) of the twelve (12) recommendations, specifically numbers 5, 6, 8, 11, and 12, and they are recommended for closure. Actions are under way to resolve the remaining items through Quarter IV, FY 2002.

The attached information is classified as "restricted" and should be exempt from disclosure under the Freedom of Information Act.

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.

Charles E. Bravo

Attachment

cc: Bob Otto
James Buie
James Golden
John Gunnels
Joyce Hansen
Robert Stephens
Gary Wetherington

475 L'Enfant Plaza SW
Washington DC 20260-2470
202 268 6000
Fax 202-268-4952
www.usps.com

Delivery Unit Notification System Application Development Review
Management Response February 19, 2002

Recommendation 1: Identify and list all critical security features by mapping existing test plans to system requirements documents, security requirements, as well as Section 508 of the Rehabilitation Act, Privacy Act of 1974, and Postal Service policies and procedures.

Response: We agree. Existing test plans will be mapped as recommended.

Schedule: April 5, 2002

Responsible Executive: Robert M. Stephens

Recommendation 2: Develop a comprehensive testing approach that would include tests of all security features.

Response: We agree. Comprehensive testing will be performed for DUNS which will include testing of all security features.

Schedule: April 5, 2002

Responsible Executive: Robert M. Stephens

Recommendation 3: Modify test plans to include tests of all security features, perform these tests, and take appropriate action(s) as required.

Response: We agree. The security test plan has been updated to include tests for all security features which will be performed. Appropriate action will be taken to resolve problems or issues indicated by test results and to incorporate those results back in to the Security Plan and Risk Assessment documents.

Schedule: April 19, 2002

Responsible Executives: Robert M. Stephens

Recommendation 4: Ensure test results are documented, retained, and approved prior to moving into the next phase of development.

Response: We agree. The DUNS project followed postal SPSP guidelines regarding documentation of test results. The results of unit and integration tests completed as of the September 17, 2001 audit date were documented, retained and provided to the OIG on September 20, 2001. Additional System, Security and Customer Acceptance Testing will be performed. Those test results will be documented, retained and approved prior to moving into the implementation phase.

Schedule: April 25, 2002

Responsible Executive: Robert M. Stephens

Recommendation 5: Ensure the business needs statement, business needs document, and requirements document are approved and provided to the development team.

Response: We agree. The business needs statement, business needs document, and requirements document were developed and signed by the portfolio manager on September 20, 2001, and copies were provided to the development team on September 21, 2001.

Closed: September 21, 2001

Responsible Executive: James W. Bule

Delivery Unit Notification System Application Development Review
Management Response February 19, 2002

Recommendation 6: Define hardware and interface requirements for the Delivery Unit Notification System once a production environment has been established.

Response: We agree. Hardware and interface requirements were defined in the Delivery Unit Notification Architectural Design document based on the initial hosting solution. A decision was recently made to host the system in the San Mateo Computer Operations Service Center and the Architectural Design document was revised on January 29 2002, to reflect the hardware and software interface requirements.

Closed: January 29, 2002.

Responsible Executive: James W. Buie

Recommendation 7: Perform system testing in an environment, which mirrors the production environment.

Response: We agree. Due to the freeze on all capital spending, we are unable to purchase hardware to replicate the production environment for testing. We are aware testing should be performed in an environment that mirrors the production environment where feasible. Since hosting for the Delivery Unit Notification system will now be provided in-house, the San Mateo COSC will temporarily assign hardware for testing purpose.

Schedule: April 12, 2002

Responsible Executive: Gary L. Wetherington

Recommendation 8: Ensure a software quality assurance representative is appointed to the Delivery Unit Notification system project.

Response: We agree. An independent software quality assurance representative was appointed to the Delivery Unit Notification system project December 14, 2001.

Closed: December 14, 2001

Responsible Executive: Robert M. Stephens

Recommendation 9: Complete a risk assessment for the Delivery Unit Notification System project, which identifies risks that may impact the cost, resources, schedule, security, and technical aspects of the project.

Response: We agree. A security risk assessment was performed for the DUNS project in accordance with the ISA process. While risks have been identified, managed and mitigated, where appropriate, throughout the development lifecycle, any remaining risks will be documented using approved risk management guidelines.

Schedule: April 12, 2002

Responsible Executive: James W. Buie

Delivery Unit Notification System Application Development Review
Management Response February 19, 2002

Recommendation 10: Ensure independent testing and validation of security requirements are performed during the information security assurance process.

Response: We agree. An independent test group will perform independent testing and validation of the security requirements. Note that independent testing and validation of security requirements are discretionary requirements in the ISA process.

Schedule: April 19, 2002

Responsible Executive: Robert M. Stephens

Recommendation 11: Designate information security assurance team members and provide them the necessary training.

Response: We agree. A designated ISA team has been established and all received training on the new ISA process on November 16, 2001.

Closed: November 16, 2001.

Responsible Executive: Robert M. Stephens

Recommendation 12: Ensure that all software used in the development effort is approved by the Infrastructure Tool Kit Requirements Committee prior to use.

Response: We agree. All software products used in Delivery Unit Notification development have been approved and are now on the Infrastructure Tool Kit. iPlanet Web Server EE v4.1 was approved July 25, 2001 and Unibar eBarz Pro was approved October 31, 2001. Both are approved for class 1.

Closed: October 31, 2001

Responsible Executive: James W. Buie