

September 27, 2002

THOMAS G. DAY
VICE PRESIDENT, ENGINEERING

CHARLES E. BRAVO
SENIOR VICE PRESIDENT, CHIEF TECHNOLOGY OFFICER

JOHN A. RAPP
SENIOR VICE PRESIDENT, OPERATIONS

SUBJECT: Audit Report – Integrated Data System Upgrade
(Report Number EM-AR-02-013)

This report presents the results of our review of the Integrated Data System Upgrade (Project Number 02BG012EM000). The self-initiated review was part of an on-going series of audits to review systems during the systems development life cycle process.

The audit disclosed that the Postal Service in-plant test plan addressed key standards and that test procedures were fully documented with expected results. However, the Postal Service did not: always involve key stakeholders in the Integrated Data System upgrade, follow the Engineering software change request process for the upgrade, complete all information security assurance requirements, and identify the hardware resources and unique network requirements for each of the Integrated Data System upgrade sites. As a result, the Postal Service upgrade may not meet customers' needs, take full advantage of the system's capabilities, adequately protect its information, and function properly at all sites.

This report made five recommendations addressing these issues. Management agreed with three of the recommendations and has planned corrective actions addressing those issues identified in this report. Management disagreed with recommendations 1 and 2. However, management's planned actions satisfy the intent of recommendation 1. The Office of Inspector General considers recommendation 2 as unresolved, but does not plan to pursue it through the formal audit resolution process. 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 audit. If you have 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: Richard J. Strasser, Jr.
Robert L. Otto
Anita J. Bizzotto
Oscar L. Avant
Charles R. Lueck
Steven N. Benson
Carole D. Koehler
George W. Wright
James L. Golden
Susan M. Duchek

TABLE OF CONTENTS

Executive Summary	i
Part I	
Introduction	1
Background	1
Objectives, Scope, and Methodology	1
Prior Audit Coverage	2
Part II	
Audit Results	3
Stakeholder Involvement	3
Recommendation	4
Management's Comments	4
Evaluation of Management's Comments	4
Software Change Request Process	5
Recommendation	5
Management's Comments	5
Evaluation of Management's Comments	6
Information Security Assurance Process	7
Recommendation	8
Management's Comments	8
Evaluation of Management's Comments	8
Hardware Resources	9
Recommendation	9
Management's Comments	10
Evaluation of Management's Comments	10
System Test Plan	11
Recommendation	11
Management's Comments	11
Evaluation of Management's Comments	11
In-Plant Test Plan	12
Appendix. Management's Comments	13

EXECUTIVE SUMMARY

Introduction

There are five major stages in the systems development life cycle.¹ Each stage has several process points that need to be accomplished to develop a successful project. This report presents our self-initiated audit of the requirements definition and testing of the Integrated Data System upgrade initiative. This is the fifth report in a series of Office of Inspector General (OIG) audits of Postal Service initiatives in the early phases of development. By early involvement in the process, the OIG can make recommendations to resolve issues 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: (1) determine if appropriate oversight took place to develop and implement the upgrade, (2) evaluate the adequacy and completeness of requirements, and (3) assess the testing phase.

Results in Brief

Our review found that: (1) key stakeholders were not always involved in the Integrated Data System upgrade, (2) the engineering software change request process for the upgrade as well as the information security assurance process was not followed, and (3) the statement of work and software requirements specification did not identify all the hardware resources. We did find, however, that the test procedures were fully documented with expected results and the in-plant test plan included key standards.

As a result, the Postal Service risks not meeting their customers' needs or taking full advantage of the systems capabilities; cannot ensure that the impact the upgrade has on resources, customers, and other systems has been identified and addressed; or that due care was taken to protect its information resources. Finally, the Postal Service is at risk that the upgraded system will not work at all sites.

Summary of Recommendations

We made 5 recommendations to correct the identified deficiencies which include ensuring: proper communication occurs with all stakeholders; program managers use the software change request process for all changes and enhancements; completion of the information security assurance requirements for the upgrade; and performance

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.

of evaluations are conducted of network infrastructure at each site prior to deployment.

**Summary of
Management's
Comments**

Management disagreed with our first two findings and recommendations and believed there was adequate stakeholder involvement and that the software change request process did not need to be followed. Management agreed with the remaining findings and recommendations and is in the process of implementing corrective actions to address those recommendations. Management's comments, in their entirety, are included in the appendix of this report.

**Overall Evaluation of
Management's
Comments**

We disagree with management's response to recommendation 2. We also believe the system upgrade should have followed the software change request process. We view the disagreement on recommendation 2 as unresolved but do not plan to pursue it through the formal audit resolution process. Management's comments are responsive to findings and recommendations 1, 3, 4, and 5. We agree with the planned corrective action for each of these recommendations.

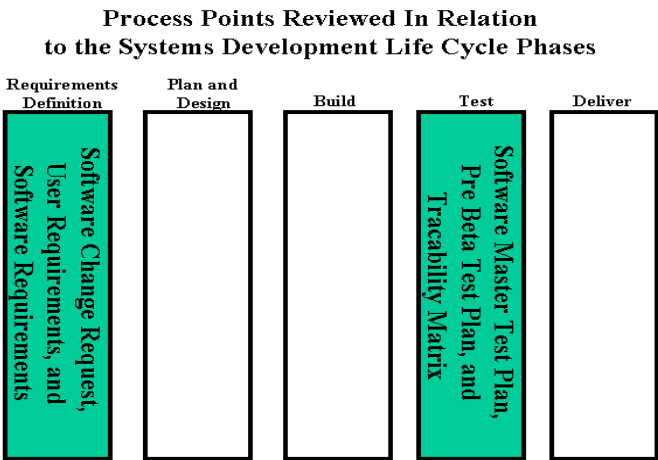
INTRODUCTION

Background

The Integrated Data System currently provides data to Confirm, a program that enables the Postal Service to share mail tracking and status information with mailers. In the future, mail processing data collected by the Integrated Data System will be used to monitor the performance of mail processing equipment. The system is currently in use at 300 Postal Service facilities.

As new programs feeding data to and relying on Integrated Data System come on-line, the system will have to handle additional data more frequently than its current capability. The estimated cost of \$34 million for the upgrade consists, in part, of \$18 million in hardware and \$10 million in software. The upgraded capability will be provided to all existing sites and 25 additional sites.

When our review took place, the Integrated Data System upgrade was at the testing phase. We reviewed both the requirements and testing phases of the project.



Objectives, Scope, and Methodology

The objectives of the Integrated Data System upgrade audit were to: (1) determine whether appropriate oversight took place to develop and implement the upgrade, (2) evaluate the adequacy and completeness of requirements, and (3) assess the testing phase.

To accomplish our objectives, we interviewed key project management personnel, including the executive sponsor,

program manager, contracting officer representative, Software Process Management personnel, and the information system security representative. In addition, we interviewed key stakeholders under the chief technology officer, Marketing, and Operations organizations. We also reviewed key documentation related to requirements, testing, and program management.

This audit was conducted from April 2002 through September 2002, and fieldwork occurred April 2002 through July 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 the objectives of this audit.

Prior Audit Coverage

We did not identify any prior audits or reviews related to the objectives of this audit.

AUDIT RESULTS

**Stakeholder
Involvement**

Key stakeholders were not always involved in the Integrated Data System upgrade project. Specifically, some of the maintenance managers at the mail processing centers were not aware of the upgrade. In addition, Confirm program management did not always participate in project decisions or review key development documents.

The Engineering methodology for software development requires all customers and users to review key development documents, such as user requirements, software requirements specification, software test plans, and in-plant test plans. The methodology also states that a field announcement should be distributed to notify users and stakeholders of software development activities. Furthermore, users and customers are members of the project change board, which is responsible for the review and disposition of all changes to a software system during its life cycle.

Engineering officials indicated that they notified a coordinator at each mail processing center concerning the upgrade. However, the information received by the coordinators was not always shared with the maintenance managers at these centers.

Confirm program management was not always involved because key program officials believed that the system upgrade had no impact on Confirm. However, we believe that Confirm program management should be involved anytime there is a change in the transmission of PLANET code data. Furthermore, Confirm program management should be considering the mailers' future expectations and how the upgrade could be used to meet their needs.

As a result of not having all key stakeholders involved, the Postal Service risks not meeting their customers' needs or taking full advantage of the system's capabilities. This may lead to additional system requirements, which could have been addressed under the current upgrade.

Recommendation	<p>We recommend the vice president, Engineering; senior vice president, Operations; and the chief technology officer, ensure:</p> <ol style="list-style-type: none">1. Proper communication occurs with all key stakeholders, including customers and users, so all relevant parties are involved in future and existing projects.
Management's Comments	<p>Management disagreed with our finding and recommendation. Management commented that the audit referenced a lack of awareness by plant managers of the upgrade as evidence of a lack of involvement. Postal Service management believes that the site surveys and the program information provided to sites was the appropriate involvement. Management stated that they can document that coordinators at each site were notified concerning the upgrade. The audit also expressed concern that mailers and members of the Confirm program group were not more intimately involved. According to management, executive managers of the upgrade were regular participants in Confirm stakeholder meetings and in monthly Confirm workgroups.</p>
Evaluation of Management's Comments	<p>Although, we agree that site coordinators were notified of the Integrated Data System upgrade, there was no involvement or feedback from the plant managers. In our view, the plant managers' input could augment the feedback from the site coordinators. We also reported that Confirm program management was not always involved in the upgrade.</p> <p>Although, management disagreed with our finding and recommendation, management's planned actions satisfy the intent of our recommendation.</p>

Software Change Request Process	<p>The Engineering software change request process was not followed for the upgrade.</p> <p>The Engineering methodology for software development establishes a software change request process, which must be followed for all enhancements or changes to software. The purpose of the software change request process is to analyze proposed changes to determine the impact and level of effort, as well as formally review projects at the project level (Project Change Board) and at the Engineering organization level (Engineering Change Board).</p> <p>The program manager did not follow the software change request process because he felt that the upgrade was primarily for hardware. Our review of the Decision Analysis Report found that the upgrade was funded in excess of \$10 million for software enhancements. In addition, the chairperson of the Engineering Change Board agreed that the project should have been reviewed and approved by the Engineering Change Board.</p> <p>As a result of not following the software change request process, the Postal Service cannot ensure that the impact the upgrade has on resources, customers, and other systems has been identified and addressed. In addition, the upgrade may not have buy-in across all levels of the Engineering organization.</p>
Recommendation	<p>We recommend the vice president, Engineering, ensure:</p> <ol style="list-style-type: none">2. Program managers are aware of the requirement to use the software change request process for all enhancements or changes to software.
Management's Comments	<p>Management disagreed with our finding and recommendation. Management stated that the contract for developing the upgrade was given to Lockheed Martin Corporation, in a competitive award. The Postal Service had an existing system in place that performed several of the functions that were included in the requirements for the upgrade. The source documents were provided to the contractor for reference. Competitors were not required to use the source documents as a basis for their proposed system upgrade work. During systems development when software systems are modified from a base of existing</p>

code and documentation then it is appropriate to impose a change management process to manage the delta. However, if the product is a new system, by definition, it is at the beginning of its lifecycle. When the contractor delivers the upgrade software to the Postal Service it is the starting point for managing changes to the delivered software and documentation baseline. Management does not believe that the change request process should have applied to this development.

**Evaluation of
Management's
Comments**

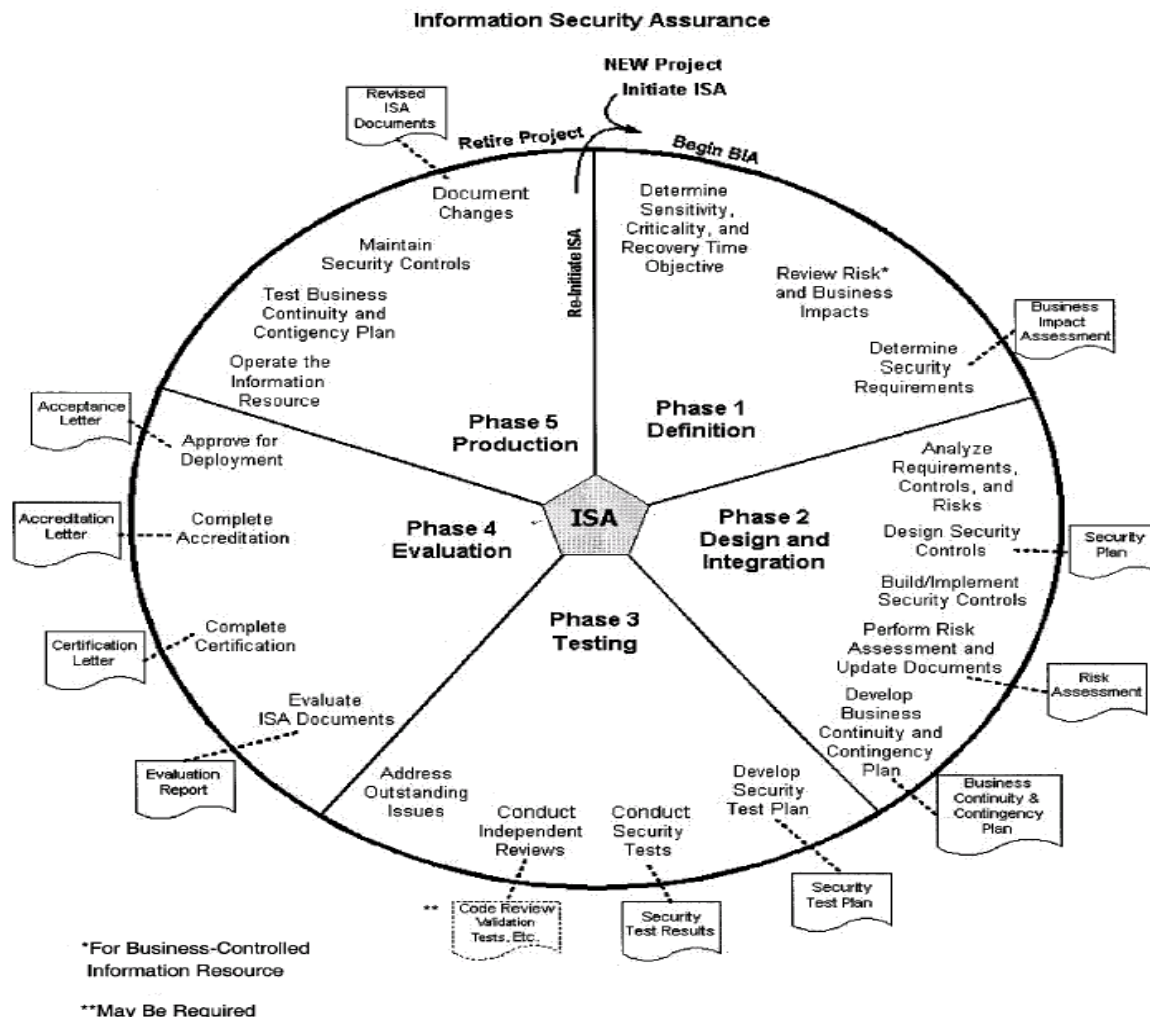
Management's comments indicate that source documents were provided for reference; but it is not stated whether the contractors used the source documents as a basis for the system. The comments did, however, state that the existing system performed several of the functions that were included in the requirements for the upgrade. Furthermore, other project documents led us to conclude this development effort was an upgrade, not a new system.

Notwithstanding this issue, we believe it is in the best interest of the Postal Service to implement our recommendation, and ensure that program managers are aware of the requirement to appropriately use the software change request process. We view the disagreement on this recommendation as unresolved but do not plan to pursue it through the formal audit resolution process.

Information Security Assurance Process

The information security assurance process outlined in Handbook AS-805² was not followed. Specifically, the business impact assessment, which includes a classification of sensitivity and criticality; the risk assessment; and security plan should have been developed prior to the current testing phase. In addition, the information system security representative did not perform the responsibilities associated with testing.

According to Handbook AS-805, the information security assurance process should be initiated anytime there are significant changes to the operating environment, the business requirements, or the application.



² The Handbook AS-805, entitled Information Security establishes the Postal Service information security policies required for appropriately identifying information resources and business requirements and appropriately protecting those information resources.

The information security assurance process requires the business impact assessment be completed in the definition phase and the risk assessment and security plan be completed in the design and integration phase (as identified on page 6 in the chart). In addition, Handbook AS-805 identifies the information system security representative's responsibilities associated with the testing phase.

The information security assurance process was not followed because the information system security representative was unaware that the information system assurance requirements had never been completed for the Integrated Data System upgrade, and that he was required to complete the requirements. He believed he was only responsible for completing the business impact assessment as part of a 3 year requirement for legacy systems. As a result of not completing the information security assurance requirements, the Postal Service cannot be assured that due care was taken to protect its information resources.

Recommendation	<p>We recommend the vice president, Engineering, ensure:</p> <p>3. The information system security representative completes the information security assurance requirements for the Integrated Data System upgrade.</p>
Management's Comments	<p>Management agreed with our finding and recommendation. Management plans to designate an information security systems representative for the Integrated Data System upgrade. The completed Information Security Assurance requirements for the Integrated Data System upgrade will be completed by November 30, 2002.</p>
Evaluation of Management's Comments	<p>In the OIG's opinion, management actions taken or planned should correct the problem or resolve the issues identified in the report.</p>

Hardware Resources

The statement of work and software requirements specification did not identify all the hardware resources. Specifically, the unique network requirements for each of the Integrated Data System upgrade sites were not identified. However, both of these documents identified equipment requirements, such as size, capacity, and memory.

The Engineering methodology for software development states that hardware resources, such as communications and network equipment, must be included in the software requirements specification.

Some hardware resources were not identified because Engineering officials did not provide all equipment and network infrastructure requirements to the vendor. In addition, they did not require the vendor to develop these requirements. Instead, Engineering decided to wait until the end of the Integrated Data System upgrade life cycle to evaluate network infrastructures at the sites.

As a result of not identifying all unique network requirements, there is a risk that the upgraded system will not work at all of the sites. Engineering officials agreed that there is an issue with the network infrastructures at some of the sites. Maintenance managers at two of the sites stated that the network infrastructures in their facilities were out-of-date and already experiencing network problems with other systems. In addition, three test sites were evaluated and it was determined that new equipment, such as switches and bridges, needed to be installed in order for the upgrade to work.

Recommendation

We recommend the vice president, Engineering, ensure:

4. An evaluation of the network infrastructure at each site prior to deployment. The evaluation should determine what enhancements are needed, there respective costs, and how they will be funded.

Management's Comments	Management agreed with our finding and recommendation. In the short term, parameters that allow for real-time interoperable exchange of data will be disabled. This is an interim measure until sufficient bandwidth becomes available. For future years, a separate initiative to upgrade the infrastructure has been prepared to request funding. Postal Service management expects this request to be before the Board of Governors in November 2002 and the upgrade would begin in early 2003 and proceed through 2006.
Evaluation of Management's Comments	In the OIG's opinion, management actions taken or planned should correct the problem or resolve the issues identified in the report.

System Test Plan	<p>The system test plan did not include the development of a security test plan, testing of security requirements, or any security considerations.</p> <p>Best practices and Handbook AS-805 state that a security test plan should be developed, which tests the security requirements. The template attached to the Engineering methodology for software development states that security considerations, such as: confidential, sensitive, or vendor-proprietary products or information, should be included in the system test plan.</p> <p>Engineering officials did not ensure the system test plan, developed by the contractor, included testing of security requirements and identification of security considerations. However, the contractor did prepare an in-plant test plan, which contained detailed test procedures related to the testing of security requirements.</p> <p>As a result of not addressing security in the system test plan, the Postal Service cannot ensure that detailed security testing procedures will be included in future test cases. In addition, the Postal Service cannot ensure that security considerations are communicated and adequately addressed during testing.</p>
Recommendation	<p>We recommend the vice president, Engineering, ensure:</p> <ol style="list-style-type: none">5. The system test plan is updated to include, at a high level, the testing of security requirements and the identification of security considerations.
Management's Comments	<p>Management agreed with our finding and recommendation. Management is currently finalizing a standardized security input document that will be issued with the statement of work. This document will be consistent with AS-805 and the Information Security Assurance process. Completion of a final document is planned for September 30, 2002.</p>
Evaluation of Management's Comments	<p>In the OIG's opinion, management actions taken or planned should correct the problem or resolve the issues identified in the report.</p>

In-Plant Test Plan

During our review of the in-plant test plan, we found that the test procedures were fully documented with expected results. In addition, the in-plant test plan included the following key standards:

- Test cases that are traceable to user, system, and software requirements.
- Measurement criteria.
- Testing of the security features.
- Testing of all requirements.
- Testing of the catastrophic recovery procedures.

APPENDIX. MANAGEMENT'S COMMENTS

THOMAS G. DAY
VICE PRESIDENT
ENGINEERING



August 8, 2002

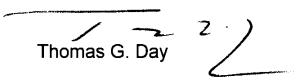
Ronald D. Merryman
Acting Assistant Inspector General
for eBusiness

SUBJECT: Response to Transmittal of Draft Audit Report – Integrated Data System
Upgrade (Report Number EM-AR-02-DRAFT)

I have attached our response to the referenced audit report. I am pleased that several of our managers met with members of your audit team to review the particulars of the report. That practice should continue.

Our responses together with your audit observations should provide a reasonably balanced view of the work done on this program. The expectation is that both the report and the response are included in any postings. In several areas we have disagreed with your observations and our explanations are included. In other areas we have agreed but our explanations describe broader factors that must be included to fully validate the observation. Where appropriate, we have included dates to accomplish needed actions. As we work together with future audits, I am certain that we will find more points of agreement.

We do not believe that there are any portions of this report that contain proprietary or other business information that must be declared exempt from FOIA. It is our intent to fully comply with the response criterion of your transmittal. Please advise if you need further information.


Thomas G. Day

Attachment

cc: Charles Bravo
John Rapp
Robert Otto
Anita Bizzotto
Steven Benson
Carole Koehler
George Wright
James Golden
Susan Duchek

Response to: OIG IDS Audit
Transmittal of Draft Audit Report – Integrated Data System Upgrade
(Report Number EM-AR 01-DRAFT)

The referenced OIG report cites several observations as a basis for recommendations concerning the development process used for the Integrated Data System. Several Engineering Managers met with the OIG for a preliminary review of their findings and addressed the issues that are cited. This report does not appear to acknowledge the clarifications that resulted from those discussions.

Our comments on the OIG findings are below:

Finding 1) Key Stakeholders were not always involved in the Integrated Data System (IDS) Upgrade.

Disagree

Comment: The Integrated Data System is an engineering system for gathering data from mail processing and material handling systems and making this data available to application clients. The IDS is NOT wedded to a particular mail transport system or marketing product. While the system will be placed in field sites, its operation is passive, will not normally require user intervention, and its impact on source data are neutral. It does not host user applications. It should be on this backdrop that we evaluate the extent of involvement appropriate for other stakeholders. The audit referenced a lack of awareness by Plant Managers of the IDS program as evidence of a lack of involvement. We believe that the site surveys and the program information descriptions provided to sites was the appropriate involvement. We can document that designated IDS coordinators at each site were notified concerning the IDS program. The audit also expressed a concern that Mailers and members of the CONFIRM Program Group were not more intimately involved. This is perhaps an audit oversight. Executive Managers of the IDS programs were regular (weekly) participants in CONFIRM stakeholder meetings and participated in the monthly CONFIRM workgroup of the Mailers Technical Advisory Committee (MTAC). It is in these meetings where any impacting changes to PLANET code and its future uses were discussed. There was not an absence of the customer's voice in the development of this product. The appropriate interface level was functional, not technical.

We do not believe that any stakeholder will claim that their interests were forfeited in the development of IDS.

Planned Actions: We will continue to work with our stakeholders to insure that we are responsive to their interest. We commit to examining how to better accomplish broader information dissemination in future programs.

Finding 2) The Engineering software change request process was not followed for the upgrade.

Disagree

Comment: The contract for developing the Integrated Data System Upgrade was given to Lockheed Martin in a competitive award. The USPS had an existing system in place that performed several of the functions that were included in the requirements for the upgrade. The source documents were provided to the contractor for reference. Competitors were NOT required to use the source documents as a basis for their proposed system upgrade work. During SDLC when software systems are modified from a base of existing code and documentation then it is appropriate to impose a change management process to manage the delta. However, if the product is a new system, by definition it is at the beginning of its lifecycle. When Lockheed Martin delivers IDS software to the USPS it is the start point for managing changes to the delivered software and documentation baseline.

As a part of contract award evaluation we reviewed Lockheed's software development process and determined it acceptable. The Engineering software change request process was never intended to impose an USPS engineering managed process on the development of new systems.

The audit references possible impacts of not following the change request process as:

- ✓ Cannot ensure impact upgrade has on resources
- ✓ Cannot ensure impact has on customers
- ✓ Cannot ensure impact has on other systems

We do not believe that the change request process should have applied to this development. The annotated concerns were appropriately addressed during the development of requirements. The appropriate process was followed.

Planned Action: None

Finding 3) The Information Security Assurance process outlined in Handbook AS-805 was not followed.

Agree

Comment: The applicable documents defining the Information Security Assurance (ISA) process are just now becoming available. We have worked closely with the Information Security Officer to support the development of this process. While it is our intent to comply fully with the applicable document, it must be recognized that these documents were in their early formative stages when the IDS contract was awarded. At that point the

complete role of the ISA process was not well understood or well published. This process matured concurrent with the development of IDS. We are now taking steps to insure that the full intent of the ISA process has been complied with. I expect that in future programs our development work will better synchronize with the defined ISA process.

We do not presently have an information systems security representative (ISSR). I assume that the conversation referenced in the audit report was with our resource assigned to security planning. This finding is fully mitigated by the fact that the documents requiring these actions are only recently available.

Planned Action: We will continue to work with the Corporate Information Security Office (CISO) to complete the Information Security Assurance (ISA) process for IDS. This will include formally designating an Information Security Systems Representative for the IDS. The Information Security Systems Representative (ISSR) for IDS will be designated by August 30. The completed Information Security Assurance requirements for IDS will be done by November 30.

Finding 4) The Statement of Work and software requirements specification did not identify all hardware resources.

Agree

Comment: This finding refers to the MPE LAN infrastructure that the Integrated Data System relies on to reliably receive data from attached MPE systems. This is a fair criticism. It identifies vulnerability that the system will have as traffic is increased on the MPE local area network. This scenario is true not just for the Integrated Data Server but also for all MPE systems that shares the use of this network. The rationale for NOT including these costs under this single program is as follows:

“The MPE local area network is shared between all mail processing systems. The cost of upgrading this shared resource should be an infrastructure cost not allocated to a particular program.”

Concurrent with developing the IDS statement of work a joint Engineering/IT separate funding initiative was developed to place structured wiring in all plants. This initiative would have fully mitigated the bandwidth issues of the MPE LAN. For budget reasons, the structured wiring initiative was not funded in FY2001 leaving the existing shared bandwidth network.

Planned Action:

In the short term, as IDS systems are installed in sites where there is intense competition for bandwidth on the MPE LAN, the parameters that allow for real-time interoperable exchange of data will be disabled. This is an interim measure until sufficient bandwidth becomes available. It allows sites to operate as is done presently with End-of-Run information. We believe that fewer than eight sites will require this. For future years, a separate initiative to upgrade the MPE LAN infrastructure has been prepared for presentation to CIC to request funding. We expect this request to be before the Board in November and that the upgrade would begin in early 2003 and proceed through 2006.

Finding 5) The system test plan did not include the development of a security test plan.

Agree

Comment: As mentioned in Finding 3, the AS-805, AS-805-G handbooks and the ISA process were not fully developed at the time of contract award. Consequently they were not available to include as a part of requirements to the contractor in developing IDS. We did send to the vendor a list of security requirements from which the vendor built a security test plan. This was discussed with the IG investigator. A copy of this list was forwarded to the IG at that time). From this list the contractor prepared a security test plan, which contained detailed test procedures related to testing security requirements. These tests were performed by the vendor at the in-plant test and reviewed by our Test and IV&V support group.

Planned Action: We are currently finalizing a standardized Security input document that will be issued with Statements of Work (SOWs). This document will be consistent with AS-805, AS-805-G and the ISA process. Representatives of Engineering, Maintenance Support, Secure Infrastructure Services (SIS), Information Systems Security Officer (ISSO) and Networks Services are participating in the workgroup to ensure consistence, completeness, and compliance with ISA requirements. Completion of a final document is planned for September 30, 2002.