

**AUDIT REPORT
13-05**

**Audit of Computer Security: GPO's Risk Acceptance Process for
Major Legacy and Minor Applications**

February 13, 2013

Date

February 13, 2013

To

Chief Information Officer

From

Inspector General

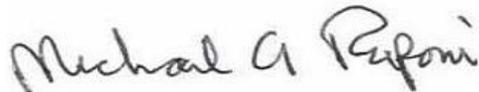
Subject

Audit of Computer Security: GPO's Risk Acceptance Process for Major Legacy and Minor Applications

Report Number 13-05

Enclosed please find the subject final report. Please refer to the "Results in Brief" for the overall audit results. Our evaluation of your response has been incorporated into the body of the report and the response is included in its entirety at Appendix B. Management either concurred or partially concurred with the recommendations. Partial concurrence was based on budgetary limitations. We consider management's comments responsive in all material aspects to the recommendations. The recommendations are resolved and will remain open pending our verification of the completion of the agreed upon actions.

We appreciate the courtesies extended to the audit staff. If you have any questions or comments about this report, please do not hesitate to contact me at (202) 512-0039.



MICHAEL A. RAPONI
Inspector General

Attachment

cc:

Acting Public Printer

Assistant Public Printer, Operations

General Counsel

Contents

Introduction	1
Results in Brief.....	3
Background	5
Results and Recommendations	7
Appendix A – Objectives, Scope, and Methodology	16
Appendix B – Management’s Response.....	18
Appendix C - Status of Recommendations	21
Appendix D - Report Distribution.....	22
Major Contributors.....	23

Office of Inspector General

Report Number 13-05

February 13, 2013

Audit of Computer Security: GPO's Risk Acceptance Process for Major Legacy and Minor Applications

Introduction

In September 2012, Information Technology & Security (IT&S) requested the Acting Public Printer accept the security risk for eight of its 16 major legacy applications. IT&S reported that none of 16 applications have completed a Certification and Accreditation (C&A). IT&S reported many of the eight major applications recommended for potential risk acceptance have been in operation for more than 20 years without any known IT security incident or fraudulent usage incident. For the remaining major legacy applications, GPO would allocate adequate resources for bringing those eight applications into full compliance with security requirements.

The eight major legacy applications support both GPO's print procurement programs and print production operations. GPO's print procurement programs provide comprehensive print procurement services to the entire federal government. The print procurement process utilizes predominately manual processes with information organized in a now aging computer mainframe environment. GPO's print production operations are configured primarily to meet the basic needs of Congress. GPO produces the daily and permanent editions — in both online and print formats — of the Congressional Record, bills, resolutions, amendments, hearings, committee reports, committee prints, documents, stationery, and a wide variety of other products. GPO is in the process of increasing efficiencies within the print procurement process and Plant Operations and is planning to reduce its reliance on existing mainframe technology.

The Acting Public Printer requested the OIG provide input into the risk acceptance request.

IT&S has primary responsibility for information technology (IT) security policy and security controls that protect the confidentiality, integrity, and availability of IT systems and data. IT&S conducts C&As. A C&A requires assessing risk, planning security, testing of minimum security controls, creating plans of actions for identified weaknesses, and mitigating risks. An authorizing officer within IT&S reviews the results of the certification and accredits the system when determining that the system's operation poses minimal security risk. GPO has 25 major applications and 206 minor applications. IT&S classified 16 of the 25 as major legacy applications. Fourteen of the 16 major legacy applications operate in a mainframe environment.

Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources, Revised, December 2000, defines a major information system as an information system requiring special management attention because of its importance to the mission of an agency; its high development, operating, or maintenance costs; or its significant role in administering agency programs, finances, property, or other resources. Major applications are by definition major information systems. According to National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004, a major application is expected to have a risk impact level of either moderate or high.

NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010, defines a minor application as any application not a major application and requiring attention to security based on the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the application. Minor applications are typically included as part of a general support system. Specific system security plans for minor applications are not required because the security controls for those applications are typically provided by the general support system or major application in which they operate. Minor applications are expected to have a risk impact level of either low or moderate.

We conducted this audit to answer the following question: "What process did GPO follow when accepting risks associated with major legacy and minor applications?"

To accomplish our audit objective, we reviewed policies and procedures in place from September to December 2012. We reviewed risk assessments and risk acceptance documentation for the eight major legacy applications IT&S reported in September 2012. To gain an understanding of policies, procedures, systems, and processes related to risk assessment and acceptance relating to IT, we conducted interviews with GPO staff to gain an understanding of applicable processes. We also interviewed key management officials responsible for establishing and monitoring the risk acceptance process; and reviewing and approving the acceptance of risk. We randomly selected four minor applications to confirm GPO's statement that C&A's and risk assessments were not conducted and we tested for the minor application's inclusion into umbrella security controls associated with either a general support system or major application.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our objective, scope, methodology, and criteria are detailed in Appendix A.

Results in Brief

GPO told us they considered the configuration of user accounts, stage of the system life cycle, years in operations without any known security incidents, sensitivity of the data stored, and monitoring results in making its risk acceptance decision.

While we agree this is important information, we also believe GPO could benefit by obtaining additional information to make a risk acceptance decision for its major legacy and minor applications. For the eight major legacy applications, our audit revealed: (1) applications were not categorized as low, moderate, or high risk based on the confidentiality, integrity, and availability of the information it stores, processes, or transmits; (2) risk assessments were not conducted assessing the sensitivity of data, threats, vulnerabilities, and effectiveness of current and/or proposed safeguards or documenting the risk assessments; and (3) risk acceptance procedures or guidelines were not fully developed. We believe this condition to be true for all 16 legacy major applications. Without categorizing, conducting risk assessments, and providing a uniform approach to risk acceptance, GPO cannot be assured that management controls in place apply the appropriate level of controls for preventing unauthorized access, use, disclosure, disruption, modification, or destruction. Factors contributing to the deficiencies noted relate to availability of resources—specifically, employees and funding. GPO reported that over the past 13 years staff supporting mainframe applications declined by 68 percent and that vacancies were not filled. According to IT&S, funding is directed toward the Federal Digital System, Passport Production System, Secure Credential Personalization System, GPO's Business Information System, Public Key Infrastructure, and the General Support System.

For minor applications, IT&S reported streamlined security reviews are conducted and the Authority to Operate process relies on continuous monitoring and change management approved by the Configuration Control Board. However, GPO could not demonstrate minor applications and subsystems with varying impact levels had adequate protection established either by major applications or general support systems. This was due to GPO's use of a streamlined security process.

If an incident were to occur, GPO could experience anywhere from minor delays to major service disruptions. For example, GPO's print procurement process relies on major legacy applications to generate random and rotating potential vendor lists for solicitations based upon order specifications, allow print procurement customers to place orders directly with a GPO contractor, format payment files to produce checks, provide order entry capability, order status, contractor performance history, quality records, exception reports, and order-tracking.

For GPO's print production operations, a senior manager told us if the Production on Estimating and Planning System, a major legacy application, were to go offline, the

impact would greatly affect GPO's ability to provide Congressional and executive agency publications.

Recommendations

To strengthen GPO's risk acceptance process, we recommend that the Chief Information Officer:

1. Categorize applications as low, moderate, or high risk based on the confidentiality, integrity, and availability of the information it stores, process, or transmits.
2. Conduct risk assessments that include, at a minimum, an assessment of the sensitivity of data, threats, vulnerabilities, and effectiveness of current/proposed safeguards, and document the risk assessments.
3. Develop procedures or guidance that adequately provide detailed instructions for risk acceptance.
4. Determine if each major application or general support system provides adequate protection to subordinate minor applications.
5. Inform business units about the exposure and potential impact on the business unit's operations if the security solution in regard to the identified risk(s) is not feasible or cannot be implemented.

Management's Response

The Chief Information Officer indicated these recommendations are reasonable activities that generally require long-term remediation actions and require a significant investment by GPO. IT&S is working to implement OIG's recommendations.

Management either concurred or partially concurred with the recommendations. Partial concurrence was based on budgetary limitations. We consider management's planned actions responsive to the recommendations. The recommendations are resolved and will remain open until planned action is complete.

Background

In a memorandum dated September 13, 2012, IT&S reported that management would accept the risk for eight of its 16 major legacy applications without conducting a C&A or having any security related documentation. For the remaining eight major applications, GPO would allocate adequate resources for bringing those eight applications into full compliance with GPO Directive 825.33B, "Information Technology Security Program Statement of Policy," May 24, 2011. The eight major legacy applications are listed below.

- Automated Bid Lists System (ABLS)
- GPO Printing Request Order Control (GPOPROC)
- Microcomp
- Paybase
- Procurement Information Control System (PICS)
- PICSWEB
- Production Estimating and Planning System (PEPS)
- Retail Order Processing System (ROPS)

In conjunction with accepting the risk for the major legacy applications, IT&S asked OIG on September 18, 2012, for closure of the following open recommendations:¹

- OIG Recommendation 10-03-04 – "Perform periodic security testing of all major applications."
- OIG Recommendation 10-03-16 – "Produce security plans for all major applications."
- OIG Recommendation 10-03-17 – "Produce risk assessments for all major applications."
- OIG Recommendation 10-03-18 – "Define required security controls and document in security plans for all major applications."
- OIG Recommendation 10-03-19 – "Certify and accredit all major applications."

IT&S noted, however, eight additional major applications for which deficiencies and recommendations still apply will continue to operate within the boundaries of GPO's current plan.

IT&S also reported streamlined security reviews are conducted for minor applications and the Authority to Operate process relies on continuous monitoring and change management approved by the Configuration Control Board.

¹ OIG Report Number 10-03, *GPO's Compliance with FISMA*, dated January 12, 2010.

Federal Security Practices

The E-Government Act of 2002 (Public Law 107-347)—passed and signed into law in December 2002—recognized the importance of information security to the economic and national security interests of the United States. Title III of that Act, entitled the Federal Information Security Management Act (FISMA), tasked NIST with the responsibility for establishing standards and guidelines. Standards and guidelines included standards for Federal agencies when categorizing information as well as information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.

Federal security practices require that agencies assess the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Both FIPS 199 and related NIST guidance provide a common framework for categorizing systems according to risk. The framework establishes three levels of potential impact on organizational operation, assets, or individuals should a breach of security occur—high (severe or catastrophic), moderate (serious), and low (limited)—and is used to determine the impact related to confidentiality, integrity, and availability.

Once determined, security categories are used with vulnerability and threat information in determining the minimum security requirements for the system and in assessing the risk to an organization. Risk assessments help ensure that the greatest risks are identified and addressed, increase the understanding of risk, and provide support for needed controls. OMB Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources,” prescribes that risk be assessed when significant changes are made to major systems and applications in an agency’s inventory, or at least every 3 years.

Consistent with NIST guidance, GPO Directive 825.33B, “Information Technology Security Program Statement of Policy,” May 24, 2011, establishes policies, assigns organizational and management roles and responsibilities, and establishes minimum requirements for development, implementation, maintenance, and oversight of an IT security program.

Although not subject to the E-Government Act of 2002, NIST Special Publications, FIPS Publications, or OMB Circulars, GPO has generally adopted those standards and operating procedures because they are not only consistent with its strategic goals but are also best business practices.

Prior OIG Audit Report

In June 2012, we reported² that strengthening security accreditation, a form of quality control, would challenge managers and technical staff at all levels to implement the most effective security controls possible for an information system. Based on the review, we noted that before authorizing a hosted Web site to operate not all elements of the C&A process were completed and recommended that GPO conduct C&A activities reflecting a risk management framework approach established in NIST Special Publication 800-37. In its management response, GPO expressed concern about the recommendation, stating that complying would have serious financial and resource implications on the Agency. As a result, management stated it would conduct a cost-benefit analysis to determine if the recommendation could be implemented within the fiscal and resource constraints of the Agency.

Results and Recommendations

GPO reported that it considered the following factors when determining the level of risk acceptance for the eight major legacy applications.

- Of the eight applications, seven are mainframe applications and by definition not Internet-facing applications, thereby reducing risk. A contracted service provider hosts GPO's mainframe applications. The service provider has both a primary site and backup site for the mainframe. IT&S stated that such a configuration significantly reduces contingency risks. In addition, mainframe applications have two separate levels of user account security, a mainframe user account, and application user account. IT&S believes the two layers of security reduce risk.
- GPO plans to retire and replace the eight major applications in the near term.
- Many of the eight major applications recommended for potential risk acceptance have been in operation at GPO for more than 20 years without any known IT security incident or fraudulent usage incident.
- Data stored and processed by applications are non-sensitive data.
- The Agency uses an on-going monitoring program that encompasses annual-user access reviews, reviews of random transactions by the specific business areas on a periodic basis, and validating a sample of transactions for completeness and lack of any issues or fraud.

While GPO considered some important information, it may benefit GPO to assess the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Our audit revealed: (1) applications were not categorized as low, moderate, or high risk based on the confidentiality, integrity, and availability of the information it stores, processes, or transmits; (2) risk assessments were not fully

² OIG Report Number 12-13, *Audit of Computer Security Handling a Denial of Service Incident*, dated June 28, 2012.

completed; and (3) risk acceptance procedures or guidelines have not been developed.

Without categorizing, conducting risk assessments, providing a uniform approach to risk acceptance, and ensuring that minor applications are protected, management was not assured that controls applied the appropriate levels to help prevent unauthorized access, use, disclosure, disruption, modification, or destruction. Management attributed deficiencies, in part, to a shortage of employees and lack of funding. For example, we were told between the early 2000's and 2013, IT staffing that supported mainframe applications went from approximately 50 to 16, a decline of 34 or 68 percent—without replacement fills for vacancies. The CIO also stated that funding to address the deficiencies in resources was not available.

Categorization of Risk. GPO did not categorize applications as low impact, moderate impact, or high impact based on the confidentiality, integrity, and availability of the information it stores, process, or transmits. Best business practices support the use of categorization.

FIPS 199 establishes security categories for Federal agencies to use in categorizing information and information systems based on the potential impact associated with the loss of confidentiality, integrity, or availability on an agency mission or individual. The publication states that systems should be categorized as low, moderate, or high based on the confidentiality, integrity, and availability of the information it stores, processes, or transmits.

NIST FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006, is the second of the security standards developed in response to FISMA and provides a minimum "foundational" level of security controls to select for protecting the confidentiality, integrity, and availability of information and systems. NIST Special Publications 800-53 Revised, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, provides 17 control families for protecting Federal information and information systems. The standard states that a selected set of security controls must include one of three appropriately tailored security control baselines from NIST Special Publication 800-53, which are associated with the designated impact levels of the organizational information systems as determined during the security categorization process.

Risk Assessment. A risk assessment is a process for analyzing and interpreting risk. A risk assessment comprises three basic activities: (1) determining the assessment's scope and methodology; (2) collecting and analyzing data; and (3) interpreting the risk analysis results. GPO did not conduct risk assessments for the 8 major applications and 4 minor applications we reviewed.

The first steps in assessing risk include identifying the system under consideration, the part of the system that will be analyzed, and the analytical method including its

level of detail and formality. The assessment may be focused on areas where either the degree of risk is unknown or is known to be high. Risk has many varying components: assets, threats, vulnerabilities, safeguards, consequences, and likelihood. This examination normally includes gathering data about the threatened area and synthesizing and analyzing the information to make it useful.

Organizations use risk assessment in support of two related functions: acceptance of risk and selection of cost-effective controls. Instances may, however, exist where a risk is so significant even after steps have been taken to mitigate, a separate risk acceptance approval by management could be appropriate.

GPO Directive 825.33B establishes policies, assigns organizational and management roles and responsibilities, and establishes minimum requirements for the development, implementation, maintenance, and oversight of an IT security program. The policy requires that management conduct risk assessments on all systems and computer installations at least once every 3 years or when a significant change occurs to the configuration of the system. IT&S Information Security must also review risk assessments annually to ensure the risks reflect the current configuration of the system or installation. Risk assessments must be in writing and include, at a minimum, sensitivity of data, threats, vulnerabilities, and effectiveness of current/proposed safeguards. Sensitivity assessments must be conducted during the initiation phase of the system's development life cycle.

Appendix III of OMB Circular A-130 requires that Federal agencies plan for security, ensure that appropriate officials are assigned security responsibilities, periodically review the security controls in their information systems, and authorize system processing prior to operations and periodically thereafter. OMB also requires reauthorization of Federal systems—or reaccreditation—at least once every 3 years through a C&A process. Certification of a system requires assessing risk, planning security, testing of minimum security controls, creating plans of actions for identified weaknesses, and mitigating risks. An authorizing officer appointed by the agency, typically a senior executive, reviews the certification results and reaccredits the system when that system's operation poses minimal security risk.

Risk Acceptance Procedures or Guidelines. Management did not develop procedures or guidelines for risk acceptance. At some point, management must decide—based on the kind of severity of remaining risks—operation of the computer system is acceptable. Managers do not always understand computer-based risk because the type of risk may be different from risks previously associated with the organization or function, the risk may be technical and difficult for a lay person to understand or the proliferation and decentralization of computing power can make it difficult to identify key assets that may be at risk.

Risk acceptance, like the selection of safeguards, should take into account various factors aside from those addressed in the risk assessment. Risk acceptance should also take into account the limitations of the risk assessment. Risk acceptance is

linked to selection of safeguards because, in some cases, risk may have to be accepted because safeguards are too expensive.

Within the Federal Government, the acceptance of risk is closely linked with an authorization to use a computer system, often called accreditation. Accreditation is management’s acceptance of risk resulting in formal approval for the system to become operational or remain so. One of the two primary functions of risk management is the interpretation of risk for the purpose of risk acceptance.

Table 1 depicts the details of the significant information available to GPO for each of eight major applications.

Table 1. Information Considered for the Risk Acceptance for the Eight Major Legacy Applications (as of January 2013)

Major Legacy Application Reviewed	C&A Completed? (Yes/No)	Risk* Assessment Completed? (Yes/No)	Categorized based on FIPS 199 as Low, Medium, or High Risk Completed? (Yes/No)	Assessment of the Sensitivity of Data Completed? (Yes/No)	Assessment of Threats Completed? (Yes/No)	Assessment of Vulnerabilities Completed? (Yes/No)	Assessment of Effectiveness of Current or Proposed Safeguards Completed? (Yes/No)
Automated Bid List System	No	Partial	No	No	No	No	No
GPO Printing Request Order Control	No	Partial	No	No	No	No	No
Microcomp	No	Partial	No	No	No	No	No
Paybase	No	Partial	No	No	No	No	No
Procurement Information Control System	No	Partial	No	No	No	No	No
Procurement Information Control System Web	No	Partial	No	No	No	No	No
Production on Estimating and Planning System	No	Partial	No	No	No	No	No
Retail Order Processing System	No	Partial	No	No	No	No	No

* Partial was assessed due to vulnerability scans conducted by GPO.

The potential business impact from the eight major legacy applications are described below.

Automated Bid List System. ABLS generates random and rotating potential vendor lists for solicitations based upon order specifications. Vendors are invited to submit bids and quotes for the solicitations. GPO has three primary methods of soliciting bids and quotes for procurements. The first method is through solicitations that are facsimiled, emailed, or physically mailed directly to qualified vendors on a rotational basis using ABLS. Even if ABLS were offline, GPO has two other methods to solicit bids and quotes for procurement. The second method is to solicit using public websites of GPO (www.gpo.gov/bidopps/index.html) and Federal Business Opportunities website (www.fedbizopps.gov). The third method is directly from the GPO Procurement Offices. Vendors or vendor's representatives may visit GPO's Central Office Bid Section in Washington, DC or any RO to view available bid opportunities. The business impact may be minimal if a secondary system is capable of providing similar functions.

GPO Printing Request Order Control. GPOPROC allows print procurement customers to place orders directly with a GPO contractor. The GPOPROC: (1) generates the purchase order, transmittal letter for the Federal agency, and letter to the vendor is generated, (2) assists with writing the printing specifications, print job requirements and contract language, and (3) searches for previous and similar orders. If GPOPROC were unavailable, the entire purchase order may be completed with ballpoint pen. This may delay procurement activities and make it difficult to gather and analyze program-wide data.

Microcomp. Microcomp is used to compose the majority of Congressional documents produced by GPO as well as key Executive agency publications. These products are printed and disseminated electronically by GPO. An estimated 700 related applications and utilities have been developed over the years to sustain and enhance Microcomp in order to support the evolving needs of GPO's Congressional customers, in-house print and electronic access. If Microcomp were offline, it may delay the production of Congressional documents as well as key Executive agency publications.

Paybase. Paybase formats payment files to produce laser checks that incorporate secure Magnetic Ink Character Recognition (MICR), printing on blank check stock; processes electronic automated clearinghouse payments; remittance generation and delivery for both paper checks and electronic payments; and digital archive and retrieval. MICR refers to the numbers printed on the bottom of the checks. If Paybase were offline, GPO may be delayed in processing payments in similar formats.

Procurement Information Control System. PICS is GPO's main information and order-tracking system used in large part to support GPO's print procurement programs. It provides order entry capability, order status, contractor performance history, quality records, and exception reports. It also integrates with GPO Proc to exchange specification details. PICS integrates with PEPS and GBIS. If PICS were offline, information and order-tracking may be delayed.

PICSWEB. PICSWEB is a web-based, user application that enables Government agencies to access the GPO PICS. PICSWEB provides customer access to central and regional office records and current job status, quality assurance information including quality level, press sheet inspection schedules and results, contractor name and address information, an estimating tool, electronic submission of 2511s (direct deal print orders only), and electronic submission of Non-Compliance Report (907). If PICSWEB were offline, GPO customers may not be able to track their print procurement orders, review quality assurance information, obtain contractor information, and access estimating tools.

Production on Estimating and Planning System. The PEPS system is used primarily to facilitate Congressional print jobs as well as print jobs for other federal agencies. GPO's plant operations relies on the PEPS to provide production estimating, scheduling, and tracking functions as well as a centralized point for data collection and record keeping for in-house production. There are between 100 -150 users of this application. Prepress, Bindery, Press would be examples of sections within GPO relying on the data in PEPS for the purpose of tracking job status as they move between divisions. If PEPS were offline, it could reduce GPO's ability to complete printing jobs for Congress and other federal agencies on schedule.

Retail Order Processing System. ROPS is part of an overall sales order system and used to expedite and control the processing of retail orders—whether keyed directly into the system or they are included through the batch process from an outside source. If the application were offline, GPO may have to manually produce picking tickets, picking lists, and customer order information notices for the acceptance of orders.

Minor Applications

IT&S reported that streamlined security reviews are conducted for minor applications and the Authority to Operate process relies on continuous monitoring and change management approved by the Configuration Control Board.

Agencies are expected to exercise judgment in determining which of their applications are minor applications and ensure that the security requirements of those applications are addressed as part of the system security plan for the applicable general support systems or, in some cases, the applicable major application. GPO could not demonstrate minor applications and subsystems had adequate protection established by major applications or general support systems.

It is common that a minor application may have a majority of its security controls provided by the general support system or major application on which it resides. In such a case, the information system owner of the general support system or major application is the information system owner for the minor application and responsible for developing the system security plan. The additional security controls specific to the minor application should be documented in the system

security plan as an appendix or paragraph. The minor application owner may develop the additional controls.

The minor application can have a FIPS 199 security category of low or moderate. However, if the minor application resides on a system that does not have adequate boundary protection, the minor application must implement the minimum baseline controls required by the host or interconnected system. Our review of four randomly selected minor applications is detailed in Table 2.

Table 2. Information Available for Four Sampled Minor Applications (as of January 2013)

Minor Application Reviewed	C&A Completed? (Yes/No)	Risk Assessment Completed? (Yes/No)	Categorized as Low, Medium, or High Risk Completed? (Yes/No)	Boundaries Established by a Major Application? (Yes/No)	Boundaries Established by a General Support System? (Yes/No)
Permanent Universal Resource Locators (PURLs)	No	No	No	No	No
Profile, Administration, Management And Library Analysis	No	No	No	No	No
Hazard (Substances) Communications System	No	No	No	No	No
GPO.gov	No	Partial*	No	No	No

* Partial was assessed due to vulnerability scans conducted by GPO.

Recommendations

To improve the effectiveness of GPO’s risk acceptance process, we recommend that the Chief Information Officer:

1. Categorize applications as low, moderate, or high risk based on the confidentiality, integrity, and availability of the information it stores, process, or transmits.
2. Conduct risk assessments that include, at a minimum, an assessment of the sensitivity of data, threats, vulnerabilities, and effectiveness of current/proposed safeguards, and document the risk assessments.
3. Develop procedures or guidance that adequately provides detailed instructions for risk acceptance.
4. Determine if each major application or general support system provides adequate protection to subordinate minor applications.

5. Inform business units about the exposure and potential impact on the business unit's operations if the security solution in regard to the identified risk(s) is not feasible or cannot be implemented.

Management's Response

Recommendation Number 1: The Chief Information Officer partially concurred. The Chief Information Officer reported this is a reasonable activity that will require commitment of additional resources to achieve. IT&S believes this can be accomplished for the major applications at GPO by December 31, 2013, with existing IT &S resources. However, the 231 minor applications at GPO cannot be completed within FY13 or by the end of FY14 without additional resources being provided to IT &S. It is estimated that that this would be completed by the end of FY14.

Recommendation Number 2: The Chief Information Officer partially concurred. The Chief Information Officer reported this is a reasonable activity that will require resource commitments to achieve. Conducting risk assessments is a component activity contained within Recommendation Number 5. It would be the most efficient overall to GPO, in the context of all the recommendations in this report, to conduct the risk assessments as part of the overall Certification and Accreditation activities in Recommendation Number 5.

Recommendation Number 3: The Chief Information Officer concurred. The Chief Information Officer reported this is a reasonable activity and IT &S estimates that it can be completed with existing IT&S resources by December 31, 2013.

Recommendation Number 4: The Chief Information Officer partially concurred. The Chief Information Officer reported this is a reasonable activity that will require additional resource commitments for IT &S. There are 231 minor applications listed on the GPO IT &S Enterprise Architecture site. IT&S estimates there is no capacity with existing IT &S resources to make the recommended determination. It is estimated that it would take 18-24 months to complete this based on the dependency on major application risk assessments and control analysis.

Recommendation Number 5: The Chief Information Officer partially concurred. IT &S believes that in order to meet this recommendation, it would be most efficient to conduct the Certification and Accreditation process for all legacy major applications. IT &S estimates that this activity would require contractor (professional service) resources to achieve and that 18-24 months of time would be needed to complete this recommendation following the NIST requirements as the OIG recommends.

Evaluation of Managements Response

The Chief Information Officer indicated these recommendations are reasonable activities that generally require long-term remediation actions and require a significant investment by GPO. IT&S is working to implement OIG's recommendations.

We consider management's planned actions responsive to the recommendations. The recommendations are resolved and will remain open until planned action is complete.

Appendix A - Objectives, Scope, and Methodology

We performed the audit from September through December 2012 at the GPO Central Office in Washington, D.C. We conducted the audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that will provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Objectives

We conducted this audit to answer the following question: “What process did GPO follow when accepting risks associated with major legacy and minor applications?”

Scope and Methodology

To meet our objectives:

- We reviewed policies and procedures in place from September to December 2012.
- We requested risk assessments and risk acceptance documentation for the eight major legacy applications reported by IT&S in September 2012.
- We randomly selected four minor applications to confirm GPO’s statement that C&A’s and risk assessments were not conducted.
- We conducted interviews with GPO staff to gain an understanding of GPO’s policies, procedures, systems, and processes related to risk assessment and acceptance as it pertains to information technology.
- We also interviewed key management officials responsible for establishing and monitoring the risk acceptance process; and reviewing and approving the acceptance of risk.

We used the results of our work to support our conclusion.

Management Controls Reviewed

We determined that the following internal controls were relevant to our audit objective:

Appendix A - Objectives, Scope, and Methodology

Program Operations – Policies and procedures the GPO management implemented to reasonably ensure that the risk acceptance process met GPO’s objectives.

Compliance with Laws and Regulations – Policies and procedures that management has implemented to reasonably ensure that resource use is consistent with laws and regulations.

The details of our examination of management controls, the results of our examination, and noted management control deficiencies are contained in the report narrative. Implementing the recommendations in this report should improve those management control deficiencies.

Appendix B – Management’s Response



U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED

Date: February 6, 2013
TO: Inspector General (IG)
FROM: Chief Information Officer (CIO)
SUBJECT: IT&S Response on Draft OIG Report 13-05:
GPO’s Risk Acceptance Process for Major Legacy and Minor Applications

Introduction

The Office of the Inspector General (OIG) issued a Draft Report 13-05 on January 14, 2013 concerning the IT&S recommendation for risk acceptance for 8 of the 16 major legacy applications and GPO’s Risk Acceptance Process for Major Legacy and Minor Applications.

This document is the official GPO Information Technology and Systems (IT&S) response to that OIG draft report in general and the recommendations contained in that Report in particular.

All of the recommendations in Draft Report 13-05 are reasonable activities. However, many of these recommendations are not achievable without the addition of significant resources. And even with the addition of resources, will take considerable time to complete. As such, IT&S has noted the conditions for disposition for each recommendation accordingly.

IT&S Response to OIG Recommendations

Recommendation #1: Categorize applications as low, moderate, or high risk based on the confidentiality, integrity, and availability of the information it stores, process, or transmits.

IT&S Response: Partially Concur.

Comments: This is a reasonable activity that will require commitment of additional resources to achieve. IT&S believes this can be accomplished for the major applications at GPO by 12/31/13 with existing IT&S resources. However, the 231 minor applications at GPO cannot be completed within FY13 or by the end of FY14 without additional resources being provided to IT&S. It is estimated that contractor (professional services) resources in the amount of \$100,000 would be required to complete this activity for the 231 minor applications at GPO and that this would be completed by the end of FY14.

Appendix B – Management’s Response

Expected Date of Disposition: 12/31/13 for Major Applications. 18 months from the date additional contractor resources are made available for Minor Applications.

Recommendation #2: Conduct risk assessments that include, at a minimum, an assessment of the sensitivity of data, threats, vulnerabilities, and effectiveness of current/proposed safeguards, and document the risk assessments.

IT&S Response: Partially Concur.

Comments: This is a reasonable activity that will require resource commitments to achieve. Conducting risk assessments is a component activity contained within Recommendation #5 below. It is estimated that conducting risk assessments for all major applications would require \$450,000 in contractor (professional services) resources for IT&S and would take approximately 6-8 months to complete. This cost estimate is included as a component within the overall total cost estimate provided below for Recommendation #5 below (since the risk assessment activity is a component of the overall activities for Recommendation #5). It would be the most efficient overall to GPO, in the context of all the recommendations in this Report, to conduct the risk assessments as part of the overall Certification and Accreditation activities in Recommendation #5.

Expected Date of Disposition: 8 months from the date additional contractor resources are made available.

Recommendation #3: Develop procedures or guidance that adequately provide detailed instructions for risk acceptance.

IT&S Response: Concur.

Comments: This is a reasonable activity to undertake. IT&S estimates that can be completed with existing IT&S resources by December 31, 2013.

Expected Date of Disposition: 12/31/13

Recommendation #4: Determine if each major application or general support system provides adequate protection to subordinate minor applications.

IT&S Response: Partially Concur.

Appendix B – Management’s Response

Comments: This is a reasonable activity that will require additional resource commitments for IT&S. There are 231 minor applications listed on the GPO IT&S Enterprise Architecture site. IT&S estimates that contractor (professional services) resources in the amount of \$200,000 would be required to perform this activity, since there is no capacity with existing IT&S resources to make the recommended determination. It is estimated that it would take 18-24 months to complete this based on the dependency on major application risk assessments and control analysis.

Expected Date of Disposition: **24 months from the date additional contractor resources are made available.**

Recommendation #5: Inform business units about the exposure and potential impact on the business unit’s operations if the security solution in regard to the identified risk(s) is not feasible or cannot be implemented.

IT&S Response: **Partially Concur.**

Comments: IT&S believes that in order to meet this recommendation, it would be most efficient to conduct the Certification and Accreditation (C&A) process for all legacy major applications. IT&S estimates that this activity would require \$1,600,000 of contractor (professional service) resources to achieve and that 18-24 months of time would be needed to complete this recommendation following the NIST requirements as the OIG recommends.

Expected Date of Disposition: **24 months from the date additional contractor resources are made available.**

Thank you for the opportunity to comment on the draft report. If you have any questions or comments about this response, or would like to discuss further, please do not hesitate to contact me at (202)512-1040.



Charles E. Riddle, Jr
Chief Information Officer

cc:
Acting Public Printer
Assistant Public Printer, Operations
General Counsel

Appendix C - Status of Recommendations

Recommendation	Resolved	Unresolved	Open/ECD*	Closed
1	x		Minor Applications: End of FY 2014 Major Applications: 12/31/2013	
2	x		8 months from the date additional contractor resources are made available	
3	x		12/31/2013	
4	x		24 months from the date additional contractor resources are made available	
5	x		24 months from the date additional contractor resources are made available	

*Estimated Completion Date.

Appendix D – Final Report Distribution

Acting Public Printer
Assistant Public Printer, Operations
General Counsel

Major Contributors to the Report

Daniel Rose, Lead Information Technology Specialist