U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

AUDIT REPORT
REPORT NUMBER 15-02

Development of a Secure Credential Production System

March 20, 2015

U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

March 20, 2015

To

Managing Director, Security and Intelligent Documents
Chief Information Officer
Director, Acquisition Services

From

Inspector General

Subject:

Audit Report—Development of a Secure Credential Production System
Report Number 15-02

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. We consider management's comments responsive to the recommendations. The recommendations are resolved and will remain open pending completion of the planned corrective actions.

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

Michael A Raponi

MICHAEL A. RAPONI
Inspector General

Attachment

cc:
Director, GPO
Deputy Director, GPO
General Counsel
Chief of Staff
Chief Administrative Officer

Contents

Office of Inspector General

Report Number 15-02 **March 20, 2015**

Development of a Secure Credential Production System

Introduction

Beginning in June 2014, GPO was the Government's sole provider of a Secure Credential Production System. Federal law requires this credential for all workers needing access to secure or restricted areas of regulated entities. Another Government agency administers the program. In May 2013, GPO entered into an Interagency Agreement to produce the secure credential. The ceiling amount of the 2-year Interagency Agreement is $7.8 million. In September 2013, GPO awarded a sole-source task order to General Dynamics Information Technology (GDIT) to provide GPO with technical integration and support services associated with development and implementation of the secure credential production system. The task order was awarded for approximately $746 thousand, with work to be completed by May 2015. GPO's Security and Intelligent Documents (SID) Business Unit is responsible for production of secure Government documents.

During testing in May 2014, GPO reported that the secure credential production system failed to process data as expected. For example, the system did not process data at an acceptable rate and the secure communication connection between GPO and another Government agency failed. Temporary card production delays were reported for June 2014. As of July 2014, GPO reported that the secure credential production system is operating in accordance with the Interagency Agreement. To GPO's credit, during the period when the production system did not meet performance requirements, GPO physically transported data via an encrypted USB [universal serial bus] flash drive in order to produce the secure credential without the secure communication connection.

This report addresses the steps GPO took to develop the secure credential production system, focusing on whether GPO adequately mitigated risks associated with the System Development Life Cycle (SDLC). We analyzed development of the production system through December 2014. We reviewed records pertaining to system development, tests performed, monitoring and approvals, configuration and technical controls, and Enterprise Architecture records. We also reviewed Federal guidance and GPO policies. We interviewed key GPO officials responsible for development and implementation of the production system.

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. See Appendix A for details of our objectives, scope, methodology, and criteria.

Results in Brief

GPO has taken numerous steps to establish an overall SDLC policy to follow when introducing a new product, system, or service. Furthermore, GPO has integrated its SDLC policy into its Information Technology (IT) Configuration Management, Enterprise Architecture (EA), and IT security policies.

At GPO[1], the Chief Information Officer (CIO) is responsible for overall management of IT resources and for establishing specific procedures and methodologies for conducting project/system development in the GPO environment. In November 2013, GPO[2] established the Technical Configuration Control Board (TCCB). The TCCB provides a forum through which GPO evaluates and monitors proposed changes to the technical environment in adherence with the SDLC. The board is responsible for reviewing and approving the technical specifications of newly proposed IT initiatives, coordinating the Phases and Gates process of technology initiatives, and addressing any major technical issue arising throughout the life cycle of an IT initiative. EA is represented on the TCCB and is responsible for ensuring that each IT request is analyzed for adherence to SDLC and the EA governance processes.

The policy further references that a Business Unit engaged in a development project must ensure adequate participation and policy compliance. For example, if SID internally manages change processes, it must be accomplished in conformance with agency process and oversight requirements specified by IT&S. Furthermore, GPO's Office of Acquisition Services (Acquisition Services) is responsible for procurement-related activities. Through its acquisition processes, GPO designates a Contracting Officer Representative (COR) that monitors, reports, and documents contractor work for GPO projects.

SID was responsible for the development of the secure credential production system. In developing the production system, SID did not follow GPO's SDLC and EA policies but rather followed an internal system development practice that SID managers told us were based on the ISO[3] 9001quality management standards for

[1] GPO Instruction 705.28, *GPO Information Technology System Development Life Cycle Policy*, dated December 12, 2005.
[2] GPO Directive 825.8, *Information Technology Configuration Management Policy*, dated November 22, 2013.
[3] ISO is the International Organization for Standardization

which SID was certified. SID managers believed they mitigated some risks by following those quality management standards.

In examining the activities associated with the development of the secure credential production system, we found that SID, IT&S, and Acquisition Services did not coordinate the development project and the following issues came to light.

- GPO project formulation policies were not followed.
- Detailed SDLC procedures were not developed.
- The SDLC framework for managing projects was not followed for 60 percent of the tasks.
- Key development Phases and Gates were not approved prior to transitioning to the next cycle and the production deployment was not approved.
- An Independent Verification and Validation (IV&V) was not performed.

In addition, we found that the COR did not provide monthly reviews of the contractor, to the contracting officer, as was required under the COR delegation letter.

As a result, GPO did not mitigate key risks associated with development of the secure credential production system, placing at risk an estimated annual revenue of $3.9 million and resulting in significant production failures as well as causing delays. Also, by not complying with the contracting officer's request for documented monthly contractor reviews, we believe GPO was at a disadvantage to take appropriate recourse against its contractor, leading us to question the $746,651 for production system support.

Recommendations

Although the production of secure credentials are at satisfactory levels, implementing the recommendations from this report should address and mitigate risks for future projects.

We recommend the Managing Director, SID, prior to the start of any future projects:

1. Coordinate with the GPO Office of Acquisitions in developing an Acquisition Plan and COR contract files and documentation requirements.

2. Coordinate with the GPO Enterprise Architecture Chief and integrate SID project architecture designs and documentation with GPO Enterprise Architecture Strategy Plan.

3. Work with IT&S when defining, implementing, and/or changing the Change Management (CM) process internal to SID to help ensure consistent establishment and maintenance of system integrity.

4. If SID follows the ISO 9001 Standard for system development, ensure that the process is conducted in conformance to GPO IT CM Policy.

We recommend the Chief Information Officer:

5. Ensure that all future IT projects, for all GPO organizations and Business Units, are analyzed for adherence to SDLC and EA governance policies.

6. Ensure that GPO Policy 705.28, *Information Technology System Development Life Cycle Policy*, December 12, 2005, is updated to reflect current operations, including section 10.a responsibilities of the Planning and Strategy Board, which no longer exists; and incorporating a mechanism for ensuring that any alternative SDLC process employed by any GPO Business Unit meets the intent of GPO Policy 705.28.

We recommend the Director, Acquisition Services:

7. Coordinate with the appropriate GPO organization and Business Unit sponsors for future projects to ensure that appointed CORs understand their responsibilities for acquisition planning and contract file documentation.

Management's Response

Management generally concurred with the recommendations. The Chief of Staff reported SID has developed, documented, and established ISO procedures for launches of new programs and products. SID is audited annually by an independent ISO auditing firm and continues to follow ISO procedures to maintain certification. SID will ensure these ISO procedures are aligned with GPO Directives or document any appropriate directive waivers that are required.

We believe GPO's planned corrective actions are responsive to the report's recommendations. The complete text of management's response is in Appendix D.

Background

GPO provides personalized smartcards and identity cards for customers throughout the Federal Government. The Secure Card Personalization System (SECAPS) is the automated system used for producing the cards. GPO developed SECAPS through a contract with GDIT. It was designed to create personalized embossed identity cards. SECAPS is GPO's automated support system for producing secure cards and credentials. GDIT supports the GPO Secure Credential Center with on-going, as-needed technical support and integration services under the Contract.

In May 2013, GPO entered into an Interagency Agreement to produce identification cards used in support of a regulated program. The program requires that complete background checks and obtain biometric identification cards to gain unescorted access to secure areas of the regulated entities. According to the Interagency Agreement, GPO must: (1) be capable of producing cards, (2) not exceed 16 hours per year of disruption to card production, (3) have a capacity to satisfy monthly card production volume surges of up to 120,000 cards per month, (4) produce cards with an average volume of 25,000 to 40,000 cards a month, (5) have an average production turnaround of 24 hours with a maximum of 48 hours (from the time the request is received), (6) personalize cards, (7) comply with security requirements, and (8) bulk mail card batches. The ceiling amount of the 2-year Interagency Agreement is $7.8 million.

In September 2013, GPO awarded GDIT a sole-source task order to provide GPO with technical integration and support services associated with development and implementation of the secure credential production system. The task order was awarded for approximately $746 thousand and work was to be completed in May 2015.

At GPO[4], the CIO is responsible for overall management of IT resources and for establishing specific procedures and methodologies for conducting project/system development in the GPO environment. In November 2013, GPO[5] established the TCCB. The TCCB provides a forum through which GPO evaluates and monitors proposed changes to the technical environment in adherence with the SDLC. The board is responsible for reviewing and approving the technical specifications of newly proposed IT initiatives, coordinating the Phases and Gates process of all technology initiatives, and addressing major technical issues that arise throughout the life cycle of any IT initiative. EA is represented on the TCCB and is responsible for ensuring IT requests are analyzed for adherence to SDLC and Enterprise Architecture governance processes. The policy further requires that the project sponsoring business unit must ensure participation and policy compliance. Thus, if

[4] GPO Instruction 705.28, *GPO Information Technology System Development Life Cycle Policy*, dated December 12, 2005.
[5] GPO Directive 825.8, *Information Technology Configuration Management Policy*, dated November 22, 2013.

SID internally manages change processes, it must be accomplished in conformance to agency processes and oversight requirements IT&S specifies. Acquisition Services is responsible for procurement-related activities such as acquisition planning and contract file documentation.

Management Control Guidelines

GPO policy requires[6] that management controls provide reasonable assurance and safeguards to protect assets against waste, loss, unauthorized use, and misappropriation. It also requires that GPO maintain effective systems of accounting and management control. The policy states that internal controls are the organization, policies, and procedures used to reasonably ensure that:

- Programs achieve intended results.
- Resources are used consistent with agency mission.
- Programs and resources are protected from waste, fraud, and mismanagement.
- Laws and regulations are followed.
- Reliable and timely information is obtained, maintained, reported, and used for decision making.

The policy further requires documentation of internal controls. Such documentation should include written policies, organization charts, procedural write-ups, manuals, memoranda, flowcharts, software, and related written materials describing the methods and measures for the internal controls and, as such, serve as a reference for individuals reviewing the internal controls and their functioning.

The Government Accountability Office (GAO) *Standards for Internal Controls in the Federal Government*, November 1999, require ongoing monitoring in the course of normal operation. Internal controls are performed continually and ingrained in an agency's operations. GAO's standards include regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties. The GAO standards also require use of control activities described as the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements or budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of Government resources and achieving effective results.

Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*, December 21, 2004 (Circular A-123), requires that managers develop and maintain effective internal controls. Effective internal

[6] GPO Instruction 825.18A, *Internal Control Program*, dated May 28, 1997.

controls provide assurance that significant weaknesses in the design or operation of internal controls that could adversely affect an agency's ability to meet its objectives would be prevented or detected in a timely manner. As a legislative branch agency, GPO is not required to follow OMB Circulars, including Circular A-123. However, because the Circular provides a sound basis for internal controls for any organization, GPO has incorporated the major requirements of Circular A-123 in its directives.

Related Audit Work

In Audit Report 11-06, *Secure Card Personalization System Information Technology Security Controls*, March 31, 2011, the OIG performed an audit of SECAPS to determine whether there was a requisite level of IT security controls in SECAPS to maintain system integrity, confidentiality, and availability. Specific audit objectives included determining the adequacy of controls associated with the SECAPS operating system, databases, physical security, system interconnections and the transmission of Personally Identifiable Information (PII), and purging of PII. We issued a report that identified opportunities to strengthen IT security controls and further reduce the potential risk of system compromise.

In Audit Report 12-19, *Enhanced Architecture Maturity Could Better Guide GPO's Transformation*, September 28, 2012, the OIG performed an audit to determine to what extent GPO had assurance that its Enterprise Architecture was used to guide and constrain ongoing development and support of GPO's strategic transformation. OIG reported that efforts to develop a fully mature Enterprise Architecture have been underway since 2008 and that GPO had developed and implemented an Enterprise Architecture policy, created the Enterprise Architecture Program Office, appointed a Chief Architect, used an automated tool that contained reference models to assist in developing an Enterprise Architecture, and established an Architect Review Board. OIG concluded that GPO had not fully expanded and evolved its Enterprise Architecture and its use for transformation and optimization and recommended, among other things, that GPO develop and implement a framework to evolve GPO's Enterprise Architecture and its use to support GPO's transformation and optimization.

Results and Recommendations

GPO established an overall SDLC framework to follow when introducing a new product, system, or service. GPO linked its SDLC policy to its Enterprise Architecture, IT Security, and IT Configuration Management, policies. For example,

- GPO Instruction 705.28 assigns organizational and management roles and responsibilities, and defines minimum requirements and procedures for implementing an IT system in support of GPO information technology projects.

- The GPO Enterprise Architecture Policy, (GPO Directive 705.31A, December 16, 2013) which has been in place since 2008,[7] provides policy to help maximize the business value of GPO's investment in IT and minimize the amount of unnecessary redundancy resulting from disparate planning, development, and IT acquisitions. The policy supports GPO's strategic vision and mission while remaining consistent with Federal and industry guidance and best practices.

- GPO Directive 825.33B, *Information Technology Security Program Statement of Policy*, dated May 24, 2011, requires a risk assessment on systems and computer installations at least once every 3 years or when a significant change has occurred to the configuration of the system. A sensitivity assessment, which is part of a risk assessment, will be conducted during the initiation phase of the system's development life cycle.

- GPO Directive 825.8, *Information Technology Configuration Management Policy*, November 22, 2013, establishes a governance policy to control changes within GPO IT plans, infrastructures, applications, services, and standards.

In March 2014, GPO conducted a pilot run of it production system. No significant failures were noted. As a result, in May 2014, GPO began its rollout of this secure credential production system at GPO's secure card production facility. During that demonstration, GPO experienced significant production failures because the system did not process data as quickly as expected nor were records able to be adequately transferred to GPO via the established secure connection. For example, the interconnection functionality failed during the project demonstration and as a result, the operator had to use a mobile storage device to manually transfer the credentials for applicants. The manual transfer of credentials for applications created a risk of either exposing or losing PII data during transit or after completion of data exchanged.

[7] The previous GPO Enterprise Architecture policy was Directive 705.31 dated December 8, 2008, which was updated to GPO Directive 705.31A on December 16, 2013.

In comparing the established framework to the activities associated with the development of the secure credential production system, we concluded that SID, IT&S, and Acquisition Services did not effectively coordinate the development project. In addition, the following issues were identified.

- Project formulation policies were not followed.
- Detailed SDLC procedures were not developed.
- The SDLC framework for managing projects was not always followed.
- Key development phases and gates were not approved prior to transitioning to the next cycle and the production deployment was not approved.
- The COR did not provide monthly reviews of the contractor.
- An IV&V was not performed.

GPO Organizations Did Not Always Coordinate Activities

In developing the secure credential production system, SID did not follow GPO's SDLC and EA policies but rather followed its internal system development practices that SID managers told us were based on the ISO 9001quality management standards for which SID was certified. SID managers stated that SID has followed that practice for all of its projects and has found that it has allowed SID to manage its projects in the most effective manner.

Because SID followed its own procedures, IT&S Officials, other than the IT Security Officer, were generally not involved in the development project. GPO policy[8] requires that business units must ensure participation and policy compliance within their respective work areas. Also, if a business unit internally manages change processes, the change must conform to agency processes and oversight requirements that IT&S specifies.

SID managers told us that in the future, they will actively participate on the TCCB and will bring to the board's attention any new initiatives.

Project Formulation Policies Not Followed

GPO did not follow project formulation policies in establishing the secure credential project. GPO policies provide project management principles and best practices to ensure that programs and projects within any GPO department or division are managed consistently toward the same goals, reducing instances of project failure and increasing the bottom line.

Directive 705.31A charges the Architecture Review Board (ARB) with, among other things, reviewing business and system initiatives for compliance with the GPO

[8] GPO Directive 825.8, *Information Technology Configuration Management Policy*, dated November 22, 2013.

Enterprise Architecture to support interoperability and data sharing and minimize redundancy.

Directive 705.28 charges the Planning and Strategy Board[9] with ensuring that GPO investment and initiatives meet the needs of the GPO mission and provide a senior administrative staff advisory role that determines high level, overall Strategic direction for guiding and prioritizing those initiatives.

We were told that SID management briefed GPO's Office of the General Counsel, Acquisition Services, the Planning and Strategy Board before the project was initiated. We were also told, SID received approval for capital purchases relative to the development project.

While we do not question whether SID received budgetary approval for the project, SID could not demonstrate it briefed the ARB or the Planning and Strategy Board as required by policy. Also, the Project Manager told us he did not engage either the ARB or the Planning and Strategy Board. The Project Manager stated that SID did not follow Directive 825.8 because SID had its own process. SID's internal change order operating procedures directed that all system design and development changes be controlled by the Engineering Change Management Committee, which was not the same as the ARB. Both design and development changes and engineering change order software changes were submitted for approval to the Engineering Change Management Committee but not the ARB.

In addition, paragraph 10.e of GPO Directive 705.28 states that either the Office of the Chief Technology Officer or the Office of the Chief Information Officer is responsible for appointing Project Managers. The SID Managing Director, and not the Chief Technology Officer or Chief Information Officer, appointed an SID Technology Program Manager as the Project Manager. The SID Managing Director stated that this has been SID's policy for all of its projects.

Detailed SDLC Procedures Were Not Developed

GPO has the framework in place requiring that programs and projects are properly approved by appropriate GPO senior managers, maximize GPO's investment in IT projects, and are managed by way of a specific and disciplined process incorporating the appropriate levels of review and approval.

However, for the secure credential production system, there was not sufficient detail in place to demonstrate a methodology—as a series of steps that could be followed—to guard against the risk of cost overruns, schedule slippage, and performance problems.

[9] Officials from GPO's Office of Programs, Strategy, and Technology stated that the Planning and Strategy Board no longer exists at GPO and that ARB assumed responsibilities for project management.

In a policy[10] dated December 2005, SDLC guidelines with detailed descriptions of required deliverables for each phase of the life cycle were to be released under a separate instruction. As of January 2015, GPO continues to draft the guidelines.

The SDLC Framework for Managing Projects Was Not Always Followed

For the SDLC processes prescribed, of the 73 required steps, GPO did not complete and document 44 (approximately 60 percent) of the steps for both the SECAPS and SECAPS/secure credential projects.

GPO, through its institutional knowledge as well as references from the National Institute of Standards and Technology and the Project Management Professionals Institute, developed a list of 73 key steps that must be completed under the first six applicable phases of a project.

GPO Instruction 705.28, which applies to the introduction of a new product, system, or service, or a significant change to an existing system or service, is a specific, disciplined process for implementing IT projects. The Instruction defines eight specific phases, with each phase having to pass through a "Gate" or formal review and approval process before a product, system or service is allowed to proceed to the next phase. Figure 1 reflects the Gates and Phases.

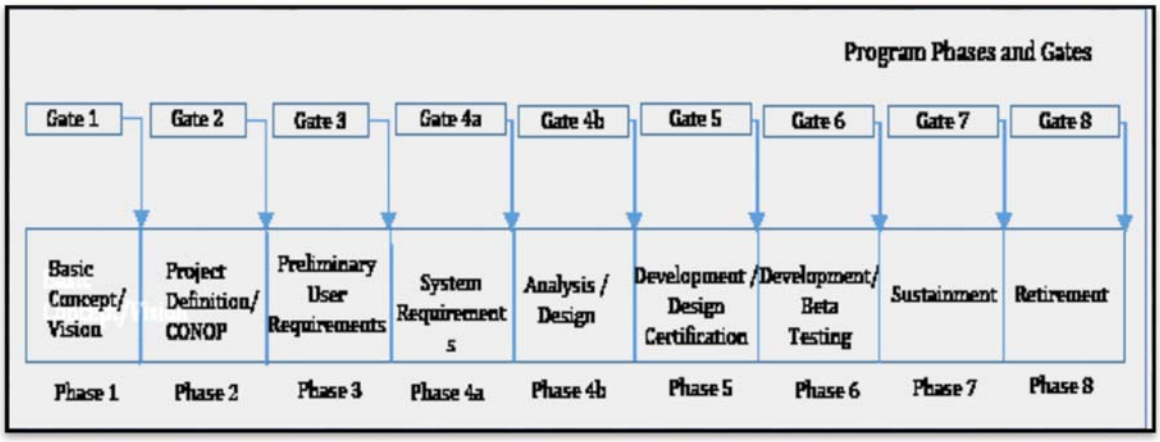

Figure 1 - SDLC Project Phases and Key Deliverables.

Below are several examples of SDLC steps not performed. See Appendix C for a detailed description.

Acquisition Planning (Phases 1 and 2). GPO could not produce a copy of an acquisition plan for the SECAPS contract or the secure credential task order. SID personnel believed that because the secure credential task order was issued in conjunction with the already-established SECAPS contract, a separate acquisition plan was not necessary. GPO officials from both Acquisitions and SID stated that

[10] GPO Instruction 705.28.

they believed an acquisition plan was developed for SECAPS, however, they could not locate it. Section 7.102 of the MMAR provides guidance for developing an acquisition plan and requires that GPO perform acquisition planning as well as conduct market research for all acquisitions to ensure that the Government meets its needs in the most effective, economical, and timely manner. Some of the MMAR-required contents of an acquisition plan that would have benefitted this task order include significant conditions affecting the acquisition, cost and performance goals, risks, and security considerations.

Project Management Planning (Phase 2 and 3). GPO did not develop a secure credential project management plan. In its listing of Federal best practices for project management,[11] GAO guidance states that project planning is the basis for controlling and managing project performance, including managing the relationship between cost and time. The guidance also states that the overall project strategy is documented in the project plan, which defines, among other things: project scope; project objectives and requirements; stakeholders; organizational and work breakdown structures; design, procurement, and implementation; and risk and opportunity management plans.

Configuration Management Plan (Phase 4). GPO did not develop a secure credential project Configuration Management Plan. In its Federal Information System Controls Audit Manual,[12] GAO requires that Federal agencies determine minimally acceptable system configuration requirements and ensure compliance with them. Systems with secure configurations have less vulnerability and are better to thwart network attacks. Configuration management plans should be developed, documented, and implemented at the entity-wide, system, and application levels to ensure an effective configuration management process. Configuration Management should be a key part of an entity's SDLC methodology.

Training Plan (Phase 5). GPO did not develop a secure credential project Training Plan. A Training Plan outlines the objectives, needs, strategy, and curriculum to be addressed when training users on the new or enhanced information system. The training plan would have ensured that the schedule account for necessary training needs to successfully implement, operate, and maintain card production. A training plan presents activities needed to support development of training materials, coordination of training schedules, reservation of personnel and facilities, planning for training needs, and other training-related tasks. Training activities are developed to teach user personnel the use of the system as specified in the training criteria.

[11] *Best Practices for Project Schedules—Exposure Draft,* GAO-12-120G (Washington, D.C.: May 30, 2012).
[12] Federal Information System Controls Audit Manual (FISCAM) – GAO-09-232G (Washington, D.C.: February 28, 2009).

Testing (All Phases). The secure credential Task Order Statement of Work states that GPO must perform complete end-to-end integration and regression testing, with GDIT, upon installation of the application, prior to System Acceptance Testing and the start of production operations. GDIT personnel stated that no complete end-to-end integration and regression testing with GPO existed prior to System Acceptance Testing. Additionally, integration and regression testing prior to System Acceptance Testing was accomplished by GDIT without GPO participation in Development, Quality Control and during staging environment.

Production Deployment Plan (Phase 6). GPO did not develop a secure credential project Production Deployment Plan. Deployment plans describe how projects would be deployed, installed, and transitioned into an operational system. A Deployment Plan would contain an overview of the secure credential system, a brief description of the major tasks involved in the deployment, the overall resources needed to support the deployment effort (such as hardware, software, facilities, materials, and personnel), and any site-specific implementation requirements. The plan is developed during the Design Phase and updated during the Development Phase. A final version of the plan is provided in the Integration and Test Phase and used for guidance during the Implementation Phase.

Key Phases, Gates, and the Production Deployment Were Not Approved

The TCCB did not approve the Phases, Gates, and the production deployment as required by GPO policy. We were told SID does not use the phases and gates process during the product development cycle, but relies on established ISO 9001 procedures to guide implementation of projects. However, SID could not provide documentation to demonstrate a waiver was granted or that GPO policy provides for a substitution similar to these circumstances.

The TCCB functions as a forum through which GPO evaluates and monitors any proposed changes to the technical environment in adherence with the SDLC. The board is responsible for reviewing and approving technical specifications of newly proposed IT initiatives, coordinating the Phases and Gates process of technology initiatives, and addresses major technical issues arising throughout the life cycle of any IT initiative. The TCCB also becomes engaged at the time of production readiness review and provides the final approval of all production deployments and changes to Production environments.

GPO's list of SDLC project phases and key deliverables requires documentation of a Phase Gate Exit at the end of each project phase to ensure proper review and approval of the completion of the phase and authorization to proceed to the next phase. The process ensures that projects proceed in accordance with the SDLC policy. GPO did not provide evidence of any Gate Exits.

Furthermore, SID did not engage the TCCB for SECAPS/secure credential project as it followed its own process involving an internal Engineering Change Management Committee.

The Contracting Officer Representatives Did Not Provide Monthly Reviews of the Contractor

The SECAPS COR did not provide monthly reviews of the contractor as the COR appointment letter requires. GPO has a process in place for appointing CORs with the technical knowledge to act for the contracting officers in the day-to-day monitoring of the contractor's performance. In the case of the SECAPS/secure credential contracts, the contracting officer appointed CORs from SID. In the COR's May 16, 2013 appointment letter (and in a subsequent June 2013 letter to a new COR), the contracting officer directed that the COR provide a monthly written review of the contractor's performance. That review was to include problems, successes, changes, or anything relevant to performance and success of the contract. The SID COR did not perform those monthly reviews. In addition, the GPO COR did not maintain sufficient contract files as the delegation letter requires.

In the aftermath of the production rollout, GPO noted several significant issues with GDIT's performance—specifically: GDIT's secure communication connection failed; GDIT missed critical agreed-upon milestones during project implementation; and GDIT's Web server connection for secure credential was unable to be thoroughly tested.

Independent Verification and Validation (IV&V) Was Not Performed

While not required, GPO did not perform an IV&V on either the SECAPS Bureau Management System or the SECAPS secure credential project. The Carnegie Mellon Software Engineering Institute—sponsored by the U.S. Department of Defense—in 2005 supported the Software IV&V as part of its Capability Maturity Model Integration Models. GPO employed the use of IV&V in previous development projects such as the Federal Digital System (FDsys).

An IV&V is performed by an independent entity that evaluates the work products generated by the team designing and/or executing a given project. An IV&V often monitors and evaluates every aspect of the project itself from inception to completion.

Recommendations

We recommend the Managing Director, SID, prior to the start of any future projects:

1. Coordinate with the GPO Office of Acquisitions in developing an Acquisition Plan and COR contract files and documentation requirements.

Management's Response. GPO Management concurs with this recommendation. SID will continue to work with Acquisitions when preparing a purchase order for any program launch. SID will ensure that the contracting officer is informed on a regular basis as to the progress of the project. The CO will be invited to contractor review meetings on a regular basis to ensure that contract performance is being monitored.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending completion of the planned actions.

2. Coordinate with the GPO Enterprise Architecture Chief and integrate SID project architecture designs and documentation with GPO Enterprise Architecture Strategy Plan.

Management's Response. GPO Management concurs with this recommendation. SID will continue to get IT involved with all program launches. IT will be involved from the start of the program through launching of each product. SID's IT manager will continue to be involved on the TCCB and will make sure any new programs initiatives are approved by the control board.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending completion of the planned actions.

3. Work with IT&S when defining, implementing, and/or changing the Change Management (CM) process internal to SID to help ensure consistent establishment and maintenance of system integrity.

Management's Response. Management concurs in general, however SID will continue to work under ISO procedures when implementing a new secure credential project. SID will work with IT on approval to follow applicable ISO procedures and implement having this as part of the applicable GPO directive.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending completion of the planned actions.

4. If SID follows the ISO 9001 Standard for system development, ensure that the process is conducted in conformance to GPO IT CM Policy.

Management's Response. Management concurs in general, however SID will continue to work under ISO procedures while ensuring IT is involved in all policy and oversight relative to overall system upgrades. In addition, SID will implement annual IT audits of the entire SECAPS system to ensure policies are consistently being followed.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending completion of the planned actions.

We recommend the Chief Information Officer:

5. Ensure that all future IT projects, for all GPO organizations and Business Units, are analyzed for adherence to SDLC and EA governance policies.

Management's Response. Management concurs in general, however referencing "all future IT projects" covers a wide variety of possible IT projects regardless of size or scope. Business Units have a responsibility to notify IT of new IT projects. If IT is not notified, it cannot perform any analysis for adherence to the established policies.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending completion of the planned actions.

6. Ensure that GPO Policy 705.28, *Information Technology System Development Life Cycle Policy*, December 12, 2005, is updated to reflect current operations, including section 10.a responsibilities of the Planning and Strategy Board, which no longer exists; and incorporating a mechanism for ensuring that any alternative SDLC process employed by any GPO Business Unit meets the intent of GPO Policy 705.28.

Management's Response. GPO Management concurs with this recommendation.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending completion of the planned actions.

We recommend the Director, Acquisition Services:

7. Coordinate with the appropriate GPO organization and Business Unit sponsors for future projects to ensure that appointed CORs understand their responsibilities for acquisition planning and contract file documentation.

Management's Response. GPO Management concurs with this recommendation.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending completion of the planned actions.

Appendix A – Objective, Scope, and Methodology

We performed fieldwork from July 2014 through January 2015 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.

Objective

The objective of the audit was to determine the steps GPO took to develop the secure credential production system, focusing on whether GPO adequately mitigated risks associated with the SDLC.

Scope and Methodology

To meet our audit objective, we analyzed development of secure credential production system through December 2014. We reviewed records pertaining to system development, tests performed, monitoring and approvals, configuration and technical controls, and Enterprise Architecture records. We also reviewed Federal guidance and GPO policies. We interviewed key GPO officials responsible for development and implementation of the secure credential production system.

Management Controls Reviewed

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

Program Operations – Policies and procedures GPO management implemented to reasonably ensure that processes met GPO's objectives.

Compliance with Laws and Regulations – Policies and procedures management implemented that reasonably ensure 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 for this audit should improve those management control deficiencies.

Computer-Generated Data. We did not rely on any computer-generated data in conducting our audit.

Appendix B – Acronyms and Abbreviations

ARB	Architecture Review Board
CM	Change Management
COR	Contracting Officer Representative
GAO	Government Accountability Office
GPO	Government Publishing Office
ISO	International Standard Organization
IT	Information Technology
IT&S	Information Technology and Systems
MMAR	Materials Management Acquisition Regulation
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identification Information
SDLC	System Development Life Cycle
SECAPS	Secure Card Personalization System
SID	Security and Intelligent Documents
TCCB	Technical Configuration Control Board

Appendix C –SDLC Project Phase Documentation

SDLC Project Phase	No Documentation	Completed
Phase 0: Business Need Analysis		
Problem Statement	**X**	
Business Case (Create) - *Partially Complete*		
Phase Gate 0 Exit	**X**	
Phase 1: Basic Concept		
Project Charter (Final)	**X**	
Funding / Budget Approval		**X**
Acquisitions / Procurement Plan	**X**	
Market Research		**X**
System Boundary Document (Final)	**X**	
Business Case (Revise) - *Partially Complete*		
Phase Gate 1 Exit	**X**	
Phase 2: Planning / Project Definition		
Standish Review	**X**	
Concept of Operations Doc - CONOPS (Create)		**X**
Acquisitions & Procurement Plan (Final)	**X**	
Project Management Plan (Create)	**X**	
Business Case (Revise) - *Partially Complete*		
Statement of Work - SOW (Create)		**X**
Phase Gate 2 Exit	**X**	
Phase 3: Functional Requirements		
Functional Requirements Document (Created)		**X**
Project Plan (Create)	**X**	
Analysis of Alternatives Documentation	**X**	
Technology Selection Documentation	**X**	
Acquisitions / Procurement	**X**	
Configuration Management Plan (Create)	**X**	
Concept of Operations Doc - CONOPS (Revise)		**X**
Project Management Plan (Revise)	**X**	
Business Case (Revise) - *Partially Complete*		
Phase Gate 3 Exit	**X**	

SDLC Project Phase	No Documentation	Completed
Phase 4: Analysis and Design		
Project Kickoff Meeting		**X**
Systems Requirements Document (Create)		**X**
Systems Requirements Traceability Matrix (Create)		**X**
System Design Document (Create)	**X**	
Training Plan (Create)	**X**	
Test Plan (Create)		**X**
Project Plan (Revise)	**X**	
Business Case (Revise) - *Partially Complete*		
Configuration Management Plan (Revise)	**X**	
Concept of Operations Doc - CONOPS (Revise)		**X**
Project Management Plan (Revise)	**X**	
Acquisitions / Procurement (Additional)	**X**	
Phase Gate 4 Exit	**X**	
Phase 5: Development and Testing		
Business Case (Final) - *Partially Complete*		
System Design Document (Finalized)	**X**	
Software Development Document (Created)	**X**	
Interface Control Document (Finalized)		**X**
Prototype / CRP / Demo	**X**	
Systems Requirements Document (Finalized)		**X**
Systems Requirements Traceability Matrix (Finalized)		**X**
Unit Testing	**X**	
Test Plan (Finalized)		**X**
Training Plan (Finalized)	**X**	
System Testing	**X**	
User Acceptance Testing		**X**
Security Review and Test		**X**
User Deployment and Communications Plans (Create)	**X**	
Implementation/Deployment Plan and Schedule (Create)		**X**
Operations and Support Plan	**X**	
Concept of Operations Doc - CONOPS (Revise)		**X**
Project Plan (Revise)	**X**	
Project Management Plan (Revise)	**X**	
Conversion Plan	**X**	
User Manual		**X**
System Administration Manual		**X**
Phase Gate 5 Exit	**X**	

SDLC Project Phase	No Documentation	Completed
Phase 6: Deployment / Implementation		
Concept of Operations Doc - CONOPS (Finalized)		**X**
Project Management Plan (Finalized)	**X**	
Software Development Document (Finalized)	**X**	
User Deployment and Communications Plans (Finalized)	**X**	
Designated Accreditation Authority (DAA) Sign-Off	**X**	
Deployment Kick-off	**X**	
Production Deployment Plan	**X**	
Delivered System	**X**	
Version Description Document		**X**
Phase Gate 6 Exit	**X**	
Phase 7: Support and Operations		
Change Control Board Reviews		**X**
User Satisfaction Reviews	**n/a**	
Justification for Retirement	**n/a**	
Financial Assessment	**n/a**	
Retirement Plan (Create)	**n/a**	
Phase Gate 7 Exit	**n/a**	
Phase 8: Retirement		
Retirement Plan (Finalized)	**n/a**	
Document Disposition	**n/a**	
System Disposition	**n/a**	
Retirement Close-out	**n/a**	
Post-Termination Review Report	**n/a**	
Phase Gate 8 Exit	**n/a**	

CONOPS – Concept of Operations
SOW – Statement of Work
DAA - Designated Accreditation Authority

Appendix D – Management's Response

Date: March 13, 2015
To: Inspector General
From: Chief of Staff
Subj: Management Response to the IG Report #15-02, "Development of a Secure Credential Production System" (March 9, 2015)

This provides management's comments on the subject report.

OBSERVATIONS

This report chronicles the development, testing, and launch of new secure credential product within SID.

When this product was launched in May 2014, SID had to closely monitor and make changes to get the program to the desired levels of performance. By mid-July 2014 SID was at projected levels of production and all issues had been addressed and resolved. Through February 2015 SID has personalized approximately 426,500 cards for this program without further problems.

SID has developed, documented, and established ISO procedures for launches of new programs and products. SID is audited annually by an independent ISO auditing firm and continues to follow ISO procedures to maintain certification. SID will ensure these ISO procedures are aligned with GPO Directives or document any appropriate directive waivers that are required.

RECOMMENDATIONS FOR SID:

1) Coordinate with the GPO Office of Acquisitions in developing an Acquisition Plan and COR contract files and documentation requirements.

RESPONSE: GPO Management concurs with this recommendation. SID will continue to work with Acquisitions when preparing a purchase order for any program launch. SID will ensure that the contracting officer is informed on a regular basis as to the progress of the project. The CO will be invited to contractor review meetings on a regular basis to ensure that contractor performance is being monitored.

2) Coordinate with the GPO Enterprise Architecture Chief and integrate project architecture design and documentation with GPO Enterprise Architecture Strategy Plan.

RESPONSE: GPO Management concurs with this recommendation. SID will continue to get IT involved with all program launches. IT will be involved from the start of the program through launching of each product. SID's IT manager will continue to be involved on the TCCB and will make sure any new programs initiatives are approved by the control board.

3) Work with IT when defining, implementing, and/or changing the Change Management (CM) process internal to the business unit to help ensure consistent establishment and maintenance of system integrity.

1

RESPONSE: Management concurs in general, however SID will continue to work under ISO procedures when implementing a new secure credential project. SID will work with IT on approval to follow applicable ISO procedures and implement having this as part of the applicable GPO directive.

4) If SID follows the ISO 9001 Standard for system development, ensure that the process is conducted in conformance to GPO IT CM Policy.

RESPONSE: Management concurs in general, however SID will continue to work under ISO procedures while ensuring IT is involved in all policy and oversight relative to overall system upgrades. In addition, SID will implement annual IT audits of the entire SECAPS system to ensure policies are consistently being followed.

RECOMMENDATIONS FOR THE CHIEF INFORMATION OFFICER:

1) **Ensure that all future IT projects, for all GPO organizations and Business Units, are analyzed for adherence to SDLC and EA governance policies.**

RESPONSE: Management concurs in general, however referencing "all future IT projects" covers a wide variety of possible IT projects regardless of size or scope. Business Units have a responsibility to notify IT of new IT projects. If IT is not notified, it cannot perform any analysis for adherence to the established policies.

2) **Ensure that GPO Policy 705.28, Information Technology System Development Life Cycle Policy, December 12, 2005, is updated to reflect current operations, including the section 10.a responsibilities of the Planning and Strategy Board, which no longer exists; and incorporating a mechanism for ensuring that any alternative SDLC process employed by any GPO Business Unit meets the intent of GPO Policy 705.28.**

RESPONSE: GPO Management concurs with this recommendation.

RECOMMENDATIONS FOR THE CHIEF, ACQUISITION SERVICES:

1) **Coordinate with the appropriate Business Unit sponsors for future projects to ensure that appointed CORs understand their responsibilities for acquisition planning and contract file documentation.**

RESPONSE: GPO Management concurs with this recommendation.

Thank you for the opportunity to provide management's response to this IG Report. If you need additional information, please do not hesitate to contact me.

ANDREW M. SHERMAN

cc: Director, GPO
Deputy Director, GPO

Chief Administrative Officer
Managing Director, Security and Intelligent Documents
Chief Information Officer
Chief, Acquisitions Service

Appendix E – Report Distribution

Director, GPO
Deputy Director, GPO
General Counsel
Chief of Staff
Chief Administrative Officer

Major Contributors to the Report

Tony Temsupasiri – Lead Information Technology Specialist
Karl Allen – Lead Auditor