U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

AUDIT REPORT
12-17

Audit of GPO's Suitability Process for Passport Production

September 18, 2012

U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

September 18, 2012

To

Managing Director for the Security and Intelligent Documents

Director of Security Services

Chief Human Capital Officer

From

Inspector General

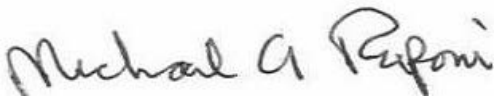
Subject

Audit Report – Audit of GPO's Suitability Process for Passport Production
Report Number 12-17

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.

We consider management's comments responsive to all of 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

Enclosure

cc:

Acting Public Printer
Assistant Public Printer, Operations
General Counsel

Contents

Introduction 1

Results in Brief 2

Background 4

Results and Recommendations 6

Appendix A – Objectives, Scope, and Methodology 12

Appendix B – Management's Response 16

Appendix C – Status of Recommendations 19

Appendix D – Report Distribution 20

Major Contributors 21

Office of Inspector General

Report Number 12-17 **September 18, 2012**

Audit of GPO's Suitability Process for Passport Production

Introduction

The Office of Inspector General (OIG) initiated an audit to examine GPO's internal processes and standards for suitability determinations of personnel that have access to Office of Security and Intelligent Documents (SID) passport production facilities.

GPO's SID has produced 65 million electronic passports in Washington, D.C. and in Mississippi. Experts agree that passport production is a critical homeland security concern, given that possession of an American passport can help a traveler bypass some of the stringent reviews conducted of those entering the U.S. from abroad. Passports can also be used by individuals as identification documents.

GPO must ensure that only trustworthy individuals have access to SID passport production facilities. The primary means for determining whether an individual is trustworthy is the background investigation, authorized by Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953, as amended and 5 C.F.R. Parts 731, 732, and 736. The background investigation is not an evaluation of the subject's character, but is instead a determination of the likelihood that a particular person will adhere to all security requirements in the future.

This audit was conducted to answer the following question: "Do opportunities exist to enhance controls over GPO's internal processes and standards for suitability determinations for personnel that have access to SID passport production facilities?"

The audit fieldwork was conducted between September 2011, through March 2012, at the GPO Central Office in Washington, D.C. To achieve our objective, we conducted interviews with key personnel security officials, human resources employees, and senior SID officials. We reviewed related laws, regulations, Executive orders, and GPO management directives. We reviewed SID guidelines and procedures, and analyzed GPO personnel security documents. We sampled 73 from a total of 244 personnel who had access to the Washington D.C. passport production facilities or who handle the passport inventory to determine if

a suitability determinations were conducted and reinvestigations were performed in accordance with GPO policies.

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 to 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 objective. Our objective, scope, methodology, and criteria are detailed in Appendix A

Results in Brief

SID is considered an important business unit for the future of GPO. We noted senior managers have worked hard to foster a culture of individual accountability to safeguard blank passports.

While senior managers are committed to mitigating risks associated with deceptive practices associated with attempting to enter the United States or used by those who seek to create a false identity, we believe controls over the personnel suitability processes could further be strengthened for passport production.

Based on our sample, we believe all 244 employees and contractors that had access to SID passport production facilities were processed for suitability determination. However, SID could strengthen its requirements process for determining which positions require clearances and level of clearances.

Periodic monitoring of employees who cleared a National Agency Check with Inquiries and Credit Check (NACIC) review is necessary. All position descriptions for employees that have access to SID should be annotated to reflect the sensitivity level of the position. We further noted that controls could be strengthened to monitor the status of reinvestigations.

Generally, these conditions occurred because: (1) SID policy does not adequately define positions requiring clearances. It states that “a limited number of SID employees spanning all the functional areas and skill sets will obtain and maintain Secret and Top Secret clearances”, (2) Position Description Forms are unclear with regard to the sensitivity level, and (3) Neither GPO or SID policy requires period monitoring

As a result, the risks for providing an avenue for potential unscrupulous activities to take place are increased.

Recommendations

We recommend that the Managing Director for the Security and Intelligent Documents Unit (1) determine the proper risk level and position classification for all employees that have access to SID passport production facilities, (2) if needed, complete the appropriate background investigations for the classification established.

We recommend that the Chief Human Capital Officer coordinate with the Managing Director for the Security and Intelligent Documents Unit and annotate position descriptions with the sensitivity level of the position.

We recommend Director of Security require employees and contractors that have access to SID passport production facilities to inform management if they are arrested, or charged with any offenses, with perhaps the exception of minor traffic infractions not involving drugs or alcohol. Also, periodically monitor cleared employees and contractors for adverse changes.

Management's Response

GPO management concurred with the recommendations.

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

Background

Since the 1920s, GPO has been the sole provider of the United States (U.S.) passport. GPO employees produce the passports in the U.S. at Secure Production Facilities (SPF) in Washington, D.C. and Mississippi. GPO is responsible for the security of blank passport production from the point at which security paper leaves the mill, through the acquisition of additional components, to the point at which the blank passport books are delivered to the Department of State. Management controls over the security related to the production of blank passports are of particular importance because travel documents, such as a blank passports, are sometimes used deceptively in attempts to enter the United States or used by those who seek to create a false identity. Also, as the sole producer of blank passports in the United States, the exposure and risk for GPO is high and could place the passport production and security document business lines at risk.

As part of passport production security, SID employees undergo a suitability determination. Suitability refers to identifiable character traits and conduct sufficient to decide whether an individual is likely or not likely to be able to carry out the duties of a job with appropriate integrity, efficiency, and effectiveness.

All positions require a risk and sensitivity designation. The highest level of risk or sensitivity determines the type of background investigation required. SID is responsible for designating risk levels for every competitive service position. These determinations are based on the position's documented duties and responsibilities. SID is to ensure that employees or contractors have the appropriate background investigation commensurate with the position and subsequent reinvestigations. There are three categories of designations applicable to SID. Each position is designated at a low, moderate, or high risk level depending on the position's potential for adverse impact to the efficiency and integrity of the service.[1] The first category or low risk level positions are non-sensitive positions involving duties and responsibilities of limited relation to an agency or program mission, so the potential for impact on the integrity and efficiency of the service is limited. Employees in these positions are subject to a NACIC.

A NACIC is the basic and minimum investigation required of all new Federal employees and contractors. It consists of searches of OPM's Security/Suitability Investigations Index,[2] the Defense Clearance and Investigations Index,[3] the

---

[1] Code of Federal Regulations (C.F.R.) § 731.106.

[2] The Security/Suitability Investigations Index includes information from the subject, interviews of other individuals in relation to him or her, and other sources such as databases, websites, etc., to verify and confirm information provided by the subject.

Federal Bureau of Investigations Name Check, the Federal Bureau of Investigations National Criminal History Fingerprint check, the Federal Bureau of Investigations Terrorist Screening Database, and other files or indices when necessary. A NACIC also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (i.e., current and past employers, schools attended, references, and local law enforcement authorities). It also includes a credit check.

The second and third categories are moderate and high risk level positions and typically referred to as "Public Trust" positions.[4] Personnel occupying public trust positions must undergo a minimum background investigation (MBI), a limited background investigation (LBI), or a background investigation.[5] Moderate risk positions within this category have the potential for moderate to serious impact on the integrity and efficiency of the service because they involve duties of considerable importance to the agency or program mission. Employees holding moderate risk public trust positions must undergo either a MBI or LBI. Positions considered to be high risk within this category have the potential for exceptionally serious impact on the integrity and efficiency of the service. The duties involved are especially critical to the agency or program mission and carry with them a broad scope of responsibility and authority. Those in high risk public trust positions must undergo a background investigation.

GPO requires that employees and contractors holding a security clearance who have been employed in their jobs for certain periods of time be subject to a reinvestigation to verify that they are still suitable for their positions. Reinvestigation is required once every 5 years for individuals possessing a Top Secret clearance, once every 10 years for individuals possessing a Secret clearance, and once every 15 years for individuals in non-sensitive positions.

As of October 2011, there were 244 individuals who had access to the Washington D.C. SPF. This number includes SID personnel; contractors; support personnel such as Quality Control and Inventory Management and maintenance; and personnel with "executive rights." The Executive staff and Security Services, which includes Physical Security and the Uniformed Police, have executive rights, allowing them access to all areas of GPO.

---

[3] The Defense Clearance and Investigation Index is composed of investigations conducted by Department of Defense investigative organizations, locator references to such investigations, and security clearances granted by Department of Defense components.

[4] Public Trust positions may involve policy-making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust.

[5] A MBI covers the same areas as a NACI, but also includes a personal subject interview. In addition to all the features of MBI, LBI includes court records verification (e.g., any felony convictions, etc.), and a check of developed references, which are the names mentioned during an investigator's talks with the references provided by the person being investigated. A background investigation features the coverage of the LBI and a check of the individual's official personnel folder.

Results and Recommendations

GPO's suitability processes are used to reduce the potential for abuse of public trust, to ensure GPO-wide uniformity and fairness for applicants, appointees, and employees, and to determine suitability for employment.

Based on our sample, we believe that all 244 employees and contractors that had access to SID passport production facilities were processed for suitability determinations. While we commend GPO on this accomplishment, we believe management controls could further be strengthened.

A sound requirements process for determining which positions require clearances and level of clearances is needed and a position designation should be annotated for all positions. Previously cleared individuals should be periodically monitored to ensure that their access to passport production facilities remains in the best interest of GPO and national security. Furthermore, controls could be strengthened to monitor the status of reinvestigations.

Generally, these conditions occurred because: (1) SID policy does not adequately define positions requiring clearances. It states that "a limited number of SID employees spanning all the functional areas and skill sets will obtain and maintain Secret and Top Secret clearances", (2) Position Description Forms are unclear with regard to the sensitivity level, and (3) Neither GPO or SID policy requires period monitoring.

As a result, the risks for providing an avenue for potential unscrupulous activities to take place are increased.

Suitability Policies and Procedures

All federal agencies must ensure that only trustworthy individuals are hired to work in national security or public trust positions. The primary means for determining whether an individual is trustworthy is the background investigation, authorized by Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953, as amended and 5 C.F.R. Parts 731, 732, and 736. The background investigation is not an evaluation of the subject's character, but is instead a determination of the likelihood that a particular person will adhere to all security requirements in the future.

GPO Directive 825.2b, "Personnel Security Program", dated February 25, 2010, states that the Director, Security Programs, is responsible for maintaining an effective personnel security program to ensure the employment and continued employment of each person is clearly consistent with the interests of national security or the public trust. The Director, Human Capital Operations, is responsible for annotating the sensitivity levels of GPO positions on appropriate personnel forms (including but not limited to the position description), and

ensuring that no individual is permanently appointed to a sensitive position until their suitability for such an appointment has been established in accordance with GPO policies. The Managing Director for the Security and Intelligent Documents Unit is responsible for determining, recording, and reporting the sensitivity level of each position under their supervision, and that action is initiated to ascertain the appropriate adjudication of selectees/appointees for such positions.

As a legislative branch agency, GPO is not required to follow any OMB circulars, including Office of Management and Budget (OMB) Circular Number A-123 "Management's Responsibility for Internal Control" or its appendixes.

OMB Circular Number A-123 requires that management controls must provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation. Management controls developed for agency programs should be logical, applicable, reasonably complete, and effective and efficient in accomplishing management objectives.

A Sound Requirements Process Reduces Security Risks

A sound requirements process for determining which positions require clearances and level of clearances is needed. The personnel security clearance process begins when a human resources or security professional determines a position's level of sensitivity, which includes consideration of whether or not a position requires access to classified information and, if required, the level of access. Current SID policies and procedures do not appear to designate position sensitivity or risk level in accordance with the risk criteria set forth in 5 CFR § 731 and § 732 and GPO Directive 825.2b, "Personnel Security Program".

GAO, in a recent study, found that a sound requirements process is necessary to "to safeguard classified data and manage costs, agencies need an effective process to determine whether civilian positions require a clearance." They also found that "underdesignating positions could lead to security risks." This is also true when positions have no designation.

SID policy letter dated June 8, 2011, titled "SID Security Clearance Program," to set policy for SID personnel security clearances. The policy requires that all passport production personnel have a suitability investigation performed. All managers, supervisors and those in leadership roles are required to have at least a secret Clearance. In addition, the policy requires that a limited number selection of employees with different skill sets and in different functional areas have a secret or top Secret clearance.

Officials believed the policy provided more flexibility and still complied with risk criteria.

A requirements process should include provisions for determining a position risk level at the high, moderate, or low risk levels. The three suitability position risk levels could be defined as follows:

- High Risk Positions involve duties that are especially critical to the agency or program mission with a broad scope of responsibility and authority, such as: policy-making, policy determining, and policy-implementing; higher level management duties and assignments, or major program responsibility; and independent spokespersons or non-management positions with authority for independent action.

- Moderate Risk Positions involve duties of considerable importance to the agency or program mission with significant program responsibility or delivery of service, such as: assistants to policy development and implementation; mid-level management duties and assignments; and delivery of service positions that demand public confidence or trust.

- Low Risk Positions involve duties and responsibilities of limited relation to an agency or program mission, so the potential for impact on the integrity and efficiency of the service is limited.

The position risk designation system described above determines the type of investigation needed for the position. Minimum investigative requirements for the position risk levels are:

High Risk – Background Investigation which consists of a Personal Subject Interview; a basic National Agency Check plus credit search; personal interviews with employment, residence, educational sources; and law enforcement searches going back 5 years.

Moderate Risk – Limited Background Investigation (LBI) or Minimum Background Investigation (MBI) may be conducted.

Low Risk –A credit search may be conducted in conjunction with a NACIC upon initial entry to duty for all appointees.

<u>Position Designation Should be Annotated for All Positions</u>

GPO Policy requires that all Position Descriptions (PD) are annotated with a sensitivity level.

Our review disclosed that Human Capital did not annotate some of the position descriptions to reflect the sensitivity level of the position. We noticed that PD's did not include sensitivity levels for "legacy" employees. Legacy employees are GPO employees that were transferred to SID when it was created. There were approximately 38 legacy employees at the time of our review. The Managing

Director of SID believes that all positions created after SID began as a separate business unit has the required annotation.

The PD is the official record of management's assignment of duties, knowledge, skills, required abilities, and supervisory relationships of the position and serves as the basis for designating suitability risk levels.

Periodic Monitoring of Cleared Employees

The favorable adjudication of a suitability determination to government or contractor employees is only one step in the protection of blank passports. Previously cleared individuals should be periodically monitored to ensure that their access to passport production remains in the best interest of GPO and national security.

Of the 73 sampled SID employees, we identified one employee and two contract personnel with information that may impact suitability. GPO policy does not specifically require employees to inform management if they are arrested, or charged with any offenses, with perhaps the exception of minor traffic infractions not involving drugs or alcohol.

Based on our sample, we estimate that there could be as many as nine instances of possible adverse activity out of the 244 employees having access to SID passport production facilities.

Controls Could be Strengthened to Monitor the Status of Reinvestigations

We determined that Security Services Clearance Tracking Program did not include all employees requiring a reinvestigation. Specifically, 40 of the 244 employees having access to SID passport production facilities were not included in the Clearance Tracking Program.

We were told that Security Services was unaware that the GPO Directive required that employees having access to SID passport production facilities in non-sensitive positions who do not have clearances also be reinvestigated every 15 years.

Without a sound requirements and monitoring process in place, GPO cannot be confident that the suitability processes in place for passport production personnel is having its intended effect.

Recommendations

We recommend Managing Director for the Security and Intelligent Documents:

1. Update SID policy and determine the proper risk level and position classification for all employees that have access to SID passport production facilities.

2. If needed, complete the appropriate background investigations for the classifications established in recommendation number 1.

Management's Response

GPO management concurred with the recommendations. The Managing Director of SID will work with the Chief Human Capital Officer to incorporate changes that result from a pending review of SID's position classifications and ensure that the position descriptions explicitly annotates any security clearance requirements. This should be completed by December 31, 2012.

We recommend the Director of Security Services:

3. Update GPO policy to require employees and contractors that have access to SID passport production facilities to inform management if they are arrested, or charged with any offenses, with perhaps the exception of minor traffic infractions not involving drugs or alcohol.

4. Periodically monitor cleared employees and contractors for adverse changes.

Management's Response.

GPO management concurred with the recommendations. The Director of Security Services will update the GPO Directive 825.2B , "Personnel Security Program" dated February 25, 2010, (Directive) to include self reporting requirements for all personnel assigned to SID (and GPO personnel assigned to support SID operations) and those having executive privileges and/or unescorted privileges to SID operations. He will also conduct and coordinate an awareness campaign and training events.

The Director of Security Services will initiate a new program to perform periodic criminal checks on SID and GPO personnel assigned to support SID operations and those having executive privileges and/or unescorted privileges to SID operations. Every five years these designated employees or contractors will be fingerprinted and subjected to background checks and monitoring for adverse changes. The Directive will be updated to include this change.

We recommend the Chief Human Capital Officer:

5. Coordinate with the Managing Director for the Security and Intelligent Documents Unit and annotate position descriptions with the sensitivity level of the position.

Management's Response.

GPO management concurred with the recommendation. The Managing Director of SID and the Chief Human Capital Officer will work together to review position descriptions and associated sensitivity levels.

Evaluation of Management's Response

Management's planned action is 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 fieldwork from September 2011 through March 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

This audit was conducted to answer the following question: "Do opportunities exist to enhance controls over GPO's internal processes and standards for suitability determinations for personnel that have access to SID passport production facilities?"

Scope and Methodology

To accomplish our audit objective, we performed the following:

- Identified and reviewed Federal and Agency personnel security policies and procedures and the GPO Memorandum of Understanding with the U.S. Department of State;
- Compared the security requirements of the Department of State MOU with those of the GPO passport vendor organizations;
- Interviewed GPO management officials and other personnel responsible for establishing and monitoring personnel security for employees working for or with the SPF. The personnel interviewed included: Managing Director, SID; the Director of Product Security, SID; Administrative Assistant, SID; Director, Security Programs; Chief, Physical Security; and Personnel Security Specialist, Physical Security; and
- The OIG investigative staff provided information on each selected employee regarding criminal activity since the date of the last clearance/background check/reinvestigation was complete or issued. The audit staff reviewed the information.

Sampling Methodology

To test whether GPO employees were in compliance with applicable personnel security policies and procedures, we randomly selected a sample of 73 from a total of 244 personnel who have access to the Washington D.C. SPF or who handle the passport inventory.

We used EZ Quant Statistical Analysis Software to support our statistical sampling. EZ Quant Statistical Analysis Software was developed by the Defense Contract Audit Agency and is used to generate sample sizes and random numbers and estimates.

Parameters

Universe Size: 244
Confidence Level: 90 percent
Sample Size: 73

Precision Limits

Lower Limit: 1.2
Upper Limit: 9.3

Below is the universe and sample by GPO Business Unit.

Universe and Sample Unit by Business Unit

Business Unit	Employees with access to SID Passport Production Facilities by Business Unit.	Sample Unit by Business Unit
Quality Control and Inventory	17	8
Uniformed Police, Physical Security and others with Executive Rights	63	25
Bindery	2	0
Building Services	3	0
Contractors	13	4
Electrical Branch	6	3
Engineering	2	0
Facilities	2	1
IT	2	1
IT-SID	1	0
Machine Branch	3	0
SID	120	30
Plant Operations	1	0
Plant Operations - SID	5	0
Security Services	1	0
Testing and Technical Services	1	0
Warehouse Operations	1	1
Warehouse Operations - SID	1	0
Total	244	73

Management Controls Reviewed

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

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

Validity and Reliability of Data – Policies and procedures that management has implemented to reasonably ensure that valid and reliable data are obtained, maintained, and fairly disclosed in reports.

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.

Computer-generated data

We did not rely on any computer-processed data from GPO's accounting or security system.

Appendix B – Management's Response

GPO

Memorandum

September 10, 2012

From: Stephen LeBlanc, Managing Director, Security and Intelligent Documents
LaMont Vernon, Director of Security Services
Ginger Thomas, Chief Human Capital Officer

To: Michael Raponi, Inspector General, Office of the Inspector General
Info: James Bradley, Assistant Public Printer for Operations

Subj: Management's Response to the Draft IG Audit Report #12-17 - dated July 26th 2012 titled Audit of GPO's Suitability Process for Passport Production

Thank you for the opportunity to respond to the draft IG Audit Report #12- 17 - dated July 26, 2012 - titled Audit of GPO's Suitability Process for Passport Production. The following response is provided for your reference and addresses the recommendations that were contained in the report:

Recommendation 1: ***Update SID policy and determine the proper risk level and position classification for all employees that have access to SID passport production facilities.***

GPO management concurs with this recommendation.
The Managing Director of SID will edit the current policy letter "SID Security Clearance Program" dated June 8th, 2011 to reference GPO Directive 825.2B, "Personnel Security Program" dated February 25, 2010. Additionally the Managing Director of SID and the Chief Human Capitol Officer will work together to incorporate changes that result from a pending review of SID's position classifications and position descriptions. The goal is to review all SID security clearances (by position classification) and ensure that the position description explicitly annotates any security clearance requirements.
Presently, all SID personnel (and GPO personnel assigned to support SID operations) are included in the Director of Security Services' Personnel Security Database which allows Security Services to track and update investigations as required. SID personnel are also tracked separately by Security Services as an extra measure to ensure these individuals remain current.
The tasks of reviewing all of SID's position classifications and position descriptions and updating the SID policy letter "SID Security Clearance Program" should be completed by December 31, 2012.

Recommendation 2: ***If needed, complete the appropriate background investigations for the classifications established in recommendation number 1.***

GPO management concurs with this recommendation.
If additional SID positions are identified that require new security clearances, those actions will be initiated through the processes and procedures managed by the Director of Security Services. These tasks will be initiated by 31 December 2012 – actual completion of the associated background and clearance investigations could take additional time based on OPM's workload and discovered issues.

Recommendation 3: ***Update GPO policy to require employees and contractors that have access to SID passport production facilities to inform management if they are arrested, or***

1

Appendix B – Management's Response

charged with any offenses, with perhaps the exception of minor traffic infractions not involving drugs or alcohol.

GPO management concurs with this recommendation.
The Director of Security Services supports this recommendation and will update the GPO Directive 825.2B, "Personnel Security Program" dated February 25, 2010 to include the self reporting requirements for all personnel assigned to SID (and GPO personnel assigned to support SID operations), and those having executive privileges and/or unescorted privileges to SID operations. To support this new self reporting requirement, the Director of Security Services will conduct and coordinate an awareness campaign and training events with the affected employees and contractors to ensure their understanding of the new policy. Additionally, the Director of Security Services and the Managing Director of SID will work with the GPO's Director of Labor Relations to ensure that the Union leadership is aware and fully briefed on the new Directive 825.2B policy change requiring self reporting for all personnel assigned to SID (and GPO personnel assigned to support SID operations), and those having executive privileges and/or unescorted privileges to SID operations.
These tasks will be initiated during September 2012 with a planned completion date of 31 December 2012.

Recommendation 4: ***Periodically monitor cleared employees and contractors for adverse changes.***

GPO management concurs with this recommendation.
The Director of Security Services will initiate a new program to perform periodic criminal checks on SID personnel (and GPO personnel assigned to support SID operations), and those having executive privileges and/or unescorted privileges to SID operations Every five (5) years these designated employees and contractors will be fingerprinted and subjected to background checks and monitoring for adverse changes. The Director of Security Services will also update the GPO Directive 825.2B, "Personnel Security Program" dated February 25, 2010 to include this new requirement for periodic five year background checks. To support this new requirement, the Director of Security Services will conduct and coordinate an awareness campaign and training events with the affected employees and contractors to ensure their understanding of the new policy. Additionally, the Director of Security Services and the Managing Director of SID will work with the GPO's Director of Labor Relations to ensure that the Union leadership is aware and fully briefed on the new Directive 825.2B policy change requiring the performance of periodic criminal checks for all personnel assigned to SID (and GPO personnel assigned to support SID operations), and those having executive privileges and/or unescorted privileges to SID operations.
These tasks will be initiated during September 2012 with a planned completion date of 31 December 2012.

Recommendation 5: ***Coordinate with the Managing Director for the Security and Intelligent Documents Unit and annotate position descriptions with the sensitivity level of the position.***

GPO management concurs with this recommendation.
The Managing Director of SID and the Chief Human Capitol Officer will work together to conduct a review of SID's position descriptions and associated sensitivity levels. The goal is to examine SID's organizational chart, position descriptions and associated sensitivity levels in order to determine and explicitly mark that position's sensitivity level.
These tasks will be completed by 31 December 2012.

Appendix B – Management's Response

Sincerely;

Stephen LeBlanc Managing Director, SID	LaMont Vernon Director of Security Services	Ginger Thomas Chief Human Capital Officer

Appendix C - Status of Recommendations

Recommendation	Resolved	Unresolved	Open/ECD*	Closed
1	x		12/31/2012	
2	x		Part 12/31/12 Part unknown based on OPM	
3	x		12/31/2012	
4	x		12/31/2012	
5	x		12/31/2012	

*Estimated Completion Date.

Appendix D - Report Distribution

Acting Public Printer
Assistant Public Printer, Operations
General Counsel

Major Contributors to the Report

Vera J. Garrant, Lead Auditor
Patricia M. Bach, Senior Auditor