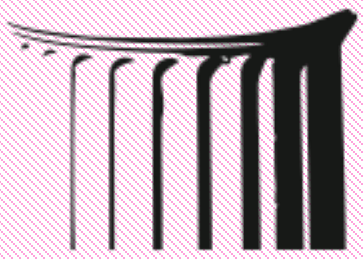

OFFICE *of*
INSPECTOR GENERAL
NATIONAL ARCHIVES

Audit of NARA's Personnel Security and Suitability Program

June 18, 2020

OIG Audit Report No. 20-AUD-12

Table of Contents

Executive Summary

Audit of NARA's Personnel Security and Suitability Program

OIG Audit Report No. 20 AUD 12 June 18, 2020

Why Did We Conduct This Audit?

A high-quality personnel security clearance process minimizes the risks of unauthorized disclosures of classified information and helps ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed. The National Archives and Records Administration's (NARA) Office of Inspector General (OIG) performed this audit to evaluate controls over the adjudication of background investigations at NARA and determine if adjudication actions were completed timely and in accordance to policy.

What Did We Recommend?

We made 15 recommendations to strengthen NARA's internal controls over its Personnel Security Program.

What Did We Find?

We found NARA's Personnel Security Policies were outdated and did not always reflect current practices, and NARA did not comply with multiple provisions of its Personnel Security policies. These conditions occurred because of a lack of monitoring and understanding of policies in place, lack of oversight of policy requirements, and inconsistency of procedures supporting the policy. As a result, NARA staff is unable to rely upon policies to guide work and may be adhering to policies no longer relevant, and the Personnel Security Program is not operating efficiently and effectively. Additionally, standard operating procedures were not documented for operations performed by Personnel Security staff. The condition occurred because Security Management did not implement internal controls for creating and maintaining procedures to guide program responsibilities. Without documented procedures, management cannot ensure a consistent and transparent process exists to support operations. Additionally, the lack of procedures result in key person dependencies and overall process inefficiencies.

We also found Security Management personnel did not: (1) did not always ensure re-investigations, pre-screening, and follow-up on submitted investigations were completed timely; (2) effectively manage the adjudication process; and (3) design and implement controls to ensure the integrity of its data in its Security Clearance Tracking System (SCTS). These conditions occurred because Security Management did not establish sufficient standard operating procedures and oversight of investigation, adjudication, and actions performed in SCTS activities. Without proper controls, NARA lacks assurance new employees are suitable for their position, current cleared employees remain suitable, and may not be able to take appropriate action to remove unsuitable staff. Additionally, there is limited assurance data in SCTS is consistent, complete, and accurately recorded for background and security investigations.

Summary of Recommendations

Finding 1: NARA Personnel Security Policies Outdated and Not Reflective of Current Practices

Number	Recommendation	Responsible Office
1	Review, update, and implement revised NARA Directive 273, *Administrative Procedures for Security Clearances*, NARA Directive 273 Supplement, *Supplement Administrative Procedures Related to Security Clearances and Applicant and Employee Rights,* NARA Directive 275, *Background and Identity Verification Process for Access Privileges,* and NARA Directive 276, *Employment or Service Suitability Determinations*.	Business Support Services

Finding 2: Noncompliance with Personnel Security Policies

Number	Recommendation	Responsible Office
2	Ensure all Security Management Personnel Security staff is familiar with updated policies.	Business Support Services
3	Implement standard formats for Human Capital notifications to Security Management Personnel Security.	Business Support Services

Finding 3: Documented Procedures Did Not Exist for Personnel Security

Number	Recommendation	Responsible Office
4	Develop and implement standard operating procedures for: position risk designations; access requirements for federal employees; background investigations; suitability and security clearance determinations; granting, suspending, or revoking security clearances; and any other aspects of the Personnel Security Program that Management determines requires standard operating procedures.	Business Support Services

Finding 4: Untimely Re-Investigations, Pre-Screening, and Follow-Up

Number	Recommendation	Responsible Office
5	Establish standards and procedures for the Personnel Security Program to ensure re-investigations, pre-screening, and follow-up on submitted investigations are completed timely.	Business Support Services

Finding 5: Lack of Control over Adjudication Decisions

Number	Recommendation	Responsible Office
6	Establish management oversight of the adjudication process, including more stringent review of serious adjudication issues with associated signoffs and documentation requirements.	Business Support Services
7	Establish standards and review procedures for adjudication decisions and report the results of the review and monitoring activities.	Business Support Services
8	Implement standard timeframes to complete adjudications.	Business Support Services
9	Implement standard response times from employees and follow-up procedures for Personnel Security.	Business Support Services
10	Implement controls to ensure adjudicator independence from cases reviewed.	Business Support Services

Finding 6: Poor Data Quality in Security Clearance Tracking System

Number	Recommendation	Responsible Office
11	The Executive for Business Support Services ensure all active NARA employees and contractor files are scanned into Security Clearance Tracking System.	Business Support Services
12	The Executive for Business Support Services establish standards and review procedures over the entry of information into Security Clearance Tracking System fields to ensure consistency and accuracy.	Business Support Services
13	The Executive for Business Support Services ensure all Security Clearance Tracking System data fields are complete and accurate for active employees.	Business Support Services
14	The Executive for Business Support Services and Chief Human Capital Officer reconcile Federal Personnel Payroll System and Security Clearance Tracking System position sensitivity ratings to ensure the two systems accurately reflect the proper sensitivity rating.	Business Support Services and Human Capital
15	The Chief Human Capital Officer, in collaboration with Business Support Services, review discrepancies in position sensitivity ratings based on the reconciliation of Federal Personnel Payroll System and Security Clearance Tracking System data, and take action to correct any position descriptions that are not classified at the proper risk level for the position.	Human Capital

Background

The National Archives and Records Administration (NARA) identifies, protects, preserves, and makes publicly available the historically valuable records of all three branches of the Federal government. NARA manages the Federal government's archives, administers a system of Presidential Libraries, operates museums, conducts education and public programs, provides oversight of government-wide records management activities, and provides temporary storage of other agencies' records on their behalf. NARA provides for the appropriate declassification of classified national security information, mediating Freedom of Information Act disputes, and overseeing agency actions regarding classified and controlled, unclassified information. As of September 2019, NARA had over 2,500 employees across its more than 40 nationwide facilities.

Background investigations of federal employees, contractors, and workers in federally regulated industries play an important role in protecting national security, employee and public safety, and vulnerable populations. Federal law requires government employees, contractors, grantees, and workers to undergo background checks to ensure their suitability for these positions. NARA follows Office of Personnel Management (OPM) regulations in Title 5 of the Code of Federal Regulations (C.F.R.) Part 732 for determining national security positions.[1] NARA also uses 5 C.F.R. Part 731 to determine employment or service suitability.

NARA's Office of Business Support Services maintains a Personnel Security Program within the Security Management Division (BX). The Personnel Security Program is led by the Personnel Security Officer (PSO). The program is responsible for developing and administering NARA personnel security policies; overseeing position risk designations for sensitivity and access requirements for federal employees in conjunction with the Office of Human Capital (Human Capital); collecting information for background investigations; making suitability and security clearance determinations; granting, suspending, or revoking security clearances; and maintaining records of clearances granted by NARA and other Federal agencies. In addition to the PSO, the program employs two personnel security specialists. Program costs for Fiscal Year (FY) 2018 and FY 2019 were $206,196 and $315,474 (estimated), respectively.

Personnel Security has used the Security Clearance Tracking System (SCTS) to manage security clearances since 2009. SCTS tracks background investigations or security investigations for all NARA employees, contractors, volunteers, and interns. SCTS documents information on NARA employees such as name, date of birth, office, position series, position sensitivity level, clearance

[1] National security positions include: (1) Those positions that involve activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and (2) Positions that require regular use of, or access to, classified information.

level, dates associated with investigation, etc. Further, SCTS stores documents related to the background investigation (e.g. OPM investigation reports, resumes, adjudication documents).

NARA investigates employees at Tier 1, Tier 2, and Tier 5 levels. Tier 1 investigations are those for positions designated as low-risk, non-sensitive and are re-investigated every 15 years. Tier 2 investigations are for non-sensitive positions designated as moderate risk public trust positions and are re-investigated every seven years. Tier 5 investigations are required for positions designated as critical sensitive, special sensitive, and/or requiring eligibility for access to Top Secret or Sensitive Compartmented Information and are re-investigated every five years. However, in 2019, NARA moved to continuous monitoring per requirements of Security Executive Agent Directive (SEAD) 6, and will now re-investigate clearance holders every seven years.

The Personnel Security Program maintains three policies and a supplement for its work:

- NARA Directive 273 (NARA 273), *Administrative Procedures for Security Clearances*, provides policies and procedures by which NARA officials request, grant, terminate, suspend, and revoke clearances for access to classified national security information at the Confidential, Secret, and Top Secret levels.
- NARA 273 also has a Supplement (NARA 273S), which further details administrative procedures for requesting and granting security clearances, terminating, suspending, and revoking security clearances and employee rights, and records management.
- NARA Directive 275 (NARA 275), *Background and Identity Verification Process for Access Privileges*, provides policies and procedures for establishing and implementing the personal identity verification, suitability, and facility and Information Technology systems access control program at NARA.
- NARA Directive 276 (NARA 276), *Employment or Service Suitability Determinations*, provides policies and procedures for implementing the background investigation and employment or service suitability process at NARA.

Human Capital is responsible for classifying position descriptions dictating position sensitivity and whether a clearance is required for the employee assigned to the position, and providing information to Personnel Security for nominees selected for appointment, promotion, or reassignment. Human Capital uses OPM's Position Designation Tool when determining position sensitivity ratings. Employee data, including individual position sensitivity ratings, is kept by Human Capital in its Federal Personnel Payroll System (FPPS). Executives, staff directors, and supervisors are responsible for ensuring accuracy of position descriptions, security clearance levels, and completion of training and other requirements. NARA clearance holders and nominees are responsible for timely response to Personnel Security, completing mandatory briefings and trainings, complying with security regulations and requirements, and reporting any changes in personal information to Personnel Security.

Objectives, Scope, Methodology

Objectives

NARA's Office of Inspector General (OIG) performed this audit to evaluate controls over the adjudication of background investigations at NARA, and determine if adjudication actions were completed timely and in accordance to policy.

Scope and Methodology

To accomplish our audit objective, we performed audit procedures at Archives II in College Park, Maryland with various NARA offices including Business Support Services, Office of Human Capital, Agency Services, Research Services, Legislative Archives, Presidential Libraries, and Museum Services, and the Insider Threat Program (ITP). The audit was performed from July 2019 to January 2020.

Specifically, we performed the following:

- Reviewed NARA 273, NARA 273S, and NARA 276 to determine policies and procedures in place, then obtained testimonial and documentary evidence as to NARA's adherence to those policies.
- Reviewed NARA 275 for continued applicability.[2]
- Reviewed relevant laws, regulations, Executive Orders, SEADs, OPM guidance, and Federal Investigative Notices.
- Reviewed processes and procedures in place for Personnel Security to include pre-screening, credit checks, investigation submission, assignments, adjudications, and SCTS entry.
- Judgmentally sampled[3] and performed various analyses of SCTS data to include:
    - Comparison of data points with FPPS including position sensitivity, office, position series, etc.
    - Tested 33 of 649 top secret clearance holders for retention of training certificates and signed Standard Form (SF)-312s, *Classified Information Nondisclosure Agreement*.

[2] Due to work performed on clearance and adjudication processes, the OIG removed NARA 275 from the scope of review.

[3] The results of our sampling cannot be projected to the intended population.

  - Reviewed compliance with volunteer procedures for the four clearance holders who retired and returned to work on classified projects.
  - Reviewed 104 FY 2019 internal transfers for required documentation and SCTS profile updates.
  - Reviewed re-investigation dates and tested timeliness for all three tiers of investigation.
- Judgmentally selected a sample of 14 of 120 new hires during FY 2019 to analyze NARA's compliance with personnel security procedures. Reviewed communication protocols between Human Capital and Personnel Security.
- Reviewed adjudications occurring from FY 2015 through FY 2019, with emphasis on those cases rated potentially disqualifying by OPM. Analyzed SCTS dates for adjudication timeliness. Reviewed investigation reports, employee files, and documentation regarding NARA's decision to adjudicate favorably or reject clearances.

Internal Controls

To assess internal controls relative to our objectives, we reviewed Business Support Services' Assurance Statement and Internal Control Program Reports for FY 2018 and FY 2019. Management reported there is reasonable assurance the management controls in Business Support Services were adequate and effective in ensuring that programs achieved their intended results. We assessed the control environment in accordance with Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* and found the controls were not adequate to ensure the program achieved intended results. Specifically, we found policies in place were either outdated, no longer reflective of current practice, or were not always complied with by Security Management. Further, NARA did not sufficiently design, establish, or maintain effective internal controls to guide program responsibilities and ensure monitoring and oversight of program operations. These internal control weaknesses are reported below.

This performance audit was conducted in accordance with generally accepted government auditing standards. The generally accepted government auditing standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by William Brown, Senior Program Auditor.

Audit Results

Finding 1. NARA's Personnel Security Policies Outdated and Not Reflective of Current Practices

NARA's Personnel Security Policies were outdated and did not always reflect current practices. The condition occurred because of a lack of monitoring by BX management and staff's understanding of policies in place. GAO's *Standards for Internal Control in the Federal Government* states management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. NARA Directive 111, *NARA Directives*, states directives are to be reviewed at least every two years from date of signature and updates coordinated. As a result, staff is unable to rely upon policies to guide work and may be adhering to policies no longer relevant.

NARA Personnel Security Policies Not Reflective of Current Practice

While NARA updated NARA 273 and NARA 273S in 2016, we found those policies are not always reflective of current practice. Specifically, we found four Parts of NARA 273[4] and three Parts of NARA 273S[5] no longer reflected current practice. Changes were made in NARA's Human Capital practices, BX Personnel Security practice, and in BX Personnel Security's response to SEADs, yet the policies were not updated to reflect these changes.

Outdated NARA Personnel Security Policies

Our review of NARA 275 and 276 found both policies were over ten years old. These policies were implemented prior to NARA's transformation in 2011, so defunct offices are given responsibilities in carrying out the policy. Further, new Executive Orders, security directives, and regulations have not been incorporated since the policies went into effect. At the start of the audit in August 2019, NARA management stated the two directives were in the process of being updated. However, as of March 2020, neither policy had been re-issued.

Recommendation

We recommend the Executive for Business Support Services:

> **Recommendation 1:** Review, update, and implement revised NARA Directive 273, *Administrative Procedures for Security Clearances*, NARA Directive 273 Supplement,

[4] Parts 273.3.e.5, 273.3.f.1.f, 273.3.h.1, and 273.3.h.2.
[5] Parts 273S.5b, 273S.9, and 273S.10.

Supplement Administrative Procedures Related to Security Clearances and Applicant and Employee Rights, NARA Directive 275, *Background and Identity Verification Process for Access Privileges,* and NARA Directive 276, *Employment or Service Suitability Determinations*.

Management Response

Business Support Services will review, update, and implement revised Directives: NARA Directive 273, Administrative Procedures for Security Clearances, NARA Directive 273 Supplement, Supplement Administrative Procedures Related to Security Clearances and Applicant and Employee Rights, NARA Directive 275, Background and Identity Verification Process for Access Privileges, and NARA Directive 276, Employment or Service Suitability Determinations. All standard operating procedures created in this action plan will be incorporated into the updated directives.

Target Completion Date: June 30, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 2. Noncompliance with Personnel Security Policies

NARA did not comply with multiple provisions of its Personnel Security policies. The condition occurred because of a lack of oversight of policy requirements, and inconsistency of procedures supporting the policy. OMB Circular A-123 states management is responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance. GAO's *Standards for Internal Control in the Federal Government* states management acts as necessary to address any deviations from the established policies. As a result, the program is not operating efficiently and effectively.

We found NARA noncompliant with four parts[6] of NARA 273: (1) The PSO was not appointed in writing;[7] (2) BX Personnel Security did not make the required notifications to the ITP; (3) NARA managers and supervisors did not always ensure accuracy of position descriptions reflecting the requirement for classified access for subordinates; and (4) NARA employees did not always provide timely response to requests from BX Personnel Security.

We also found NARA was noncompliant with eight parts[8] of NARA 273S: (1) Human Capital and its shared services provider did not consistently provide all data to BX Personnel Security during the hiring process for external hires; (2) Human Capital and its shared services provider provided more information than necessary for internal hires sampled during FY 2019; (3) Human Capital onboarded an employee before the PSO pre-screened the applicant; (4) Written requests for retirees to keep security clearances when returning to NARA were not consistently maintained in SCTS; (5) Documentation for employees transferring between NARA units was not consistently maintained in SCTS; (6) Training certificates and signed SF-312s were not consistently maintained in SCTS; (7) One employee had an unsigned SF-312 in their file with no documentation maintained as to why the employee did not sign; and (8) BX Personnel Security had multiple issues with missing, incorrect, or misplaced records.

Recommendations

We recommend the Executive for Business Support Services:

Recommendation 2: Ensure all Security Management Personnel Security staff is familiar with updated policies.

Management Response

Business Support Services will ensure all Security Management Personnel Security staff are familiar with updated policies. Once the directives are updated and issued we will

[6] Parts 273.3.b (3), 273.3.f. (1) (b), 273.3.f (1) (b), and 273.3.j (1).

[7] The Executive for Business Support Services appointed the PSO in writing when brought to management's attention during the audit.

[8] Parts 273S.2.a (1), 273S.2.a (2), 273S.2.c, 273S.6, 273S.11.b, 273S.12.b, 273S.12.c, and 273S.23.

have staff read them and sign a statement that they understand and will follow the policy(s).

Target Completion Date: June 30, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 3: Implement standard formats for Human Capital notifications to Security Management Personnel Security for internal and external hires.

Management Response

Business Support Services will create a standardized form that will outline the required information Security Management Personnel Security needed from Human Capital.

Target Completion Date: December 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 3. Documented Procedures did not exist for Personnel Security

Standard operating procedures were not documented for operations performed by BX Personnel Security staff. The condition occurred because BX did not implement internal controls for creating and maintaining procedures to guide program responsibilities. GAO's *Standards for Internal Control in the Federal Government* states those in key roles for the unit may further define policies through day-to-day procedures. NARA 273 states the PSO develops and implements policies, procedures, standards, and requirements for determining the initial and continuing review of personnel for access to classified information. Without documented procedures, management cannot ensure a consistent and transparent process exists to support operations. Additionally, the lack of procedures result in key person dependencies and overall process inefficiencies.

While NARA implemented policies (NARA 273, 273S, 275, and 276) for its Personnel Security Program, it lacked written standard operating procedures to support program operations. Procedures were communicated verbally to staff, shared informally through emails, or learned through on-the-job experience. Also, staff relied upon knowledge shared by seasoned employees and the experience of staff to perform job duties.

For example, a former PSO developed a brief procedure on the process for a top secret clearance. While this document outlined many steps in the process, we found it to be incomplete as not all steps in the process were included or fully developed. BX Personnel Security staff was aware the document existed, but did not use it. Instead, staff relied on their personally-created procedure documents in lieu of the procedure created by the PSO or an office-wide procedure. These procedure documents were developed based on staff's own knowledge and understanding of the processes as explained verbally to them.

We found the PSO to be familiar and knowledgeable on the many actions and responsibilities required of the role, including personnel security processes and specific actions taken within the process. However, in many cases, no documentary evidence existed to outline those processes and actions performed by the PSO. If the PSO were to leave the agency without sufficiently documenting processes used, the loss of the knowledge and familiarity of the program would be detrimental to the agency.

Recommendations

We recommend the Executive for Business Support Services:

> **Recommendation 4:** Develop and implement standard operating procedures for: position risk designations; access requirements for federal employees; background investigations; suitability and security clearance determinations; granting, suspending, or

revoking security clearances; and any other aspects of the Personnel Security Program that Management determines requires standard operating procedures.

Management Response

Business Support Services will develop and implement standard operating procedures for: position risk designations; access requirements for federal employees; background investigations; suitability and security clearance determinations; granting, suspending, or revoking security clearances.

Target Completion Date: December 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 4. Untimely Re-Investigations, Pre-Screening and Follow-Up

BX did not always ensure re-investigations, pre-screening, and follow-up on submitted investigations were completed timely. The condition occurred because BX did not establish sufficient standard operating procedures and oversight of investigation activities. GAO's *Standards for Internal Control in the Federal Government* management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. NARA 273 states the PSO manages the personnel security program, and monitors on-going investigations. Therefore, NARA lacks assurance: (1) current cleared employees should continue to have access to classified information; (2) all applicants have the necessary background investigation for their position; and (3) submitted investigations are proceeding timely.

NARA's Personnel Security program has many different tasks and processes associated with the responsibilities of the unit including pre-screening applicants, submitting investigation requests to investigation agencies, reviewing investigation reports, granting security clearances, ensuring employee suitability, and tracking cleared employees' need for re-investigation. In review of those processes, we found:

- Untimely Re-investigations – BX receives annual reports from its SCTS contractor on upcoming re-investigations for Tier 1 and Tier 5 employees, but not for Tier 2 re-investigations. As a result, some Tier 2 re-investigations were not timely initiated. Also, despite the receipt of annual reports for Tier 1 and Tier 5 re-investigations, BX was not always timely re-investigating employees at those levels.
- 24-hour Pre-Screening Investigation Response – The PSO monitored the 24-hour response time for hiring requests manually and did not keep the results. While most responses occurred within the 24-hour period, in one instance the PSO did not pre-screen an applicant for a Tier 1 position before Human Capital onboarded the employee.
- Investigation Follow-Up – BX does not maintain built-in processes to follow-up with the investigating agency at certain intervals in background investigations. We found examples of cases where the completed investigation is not submitted to BX timely and months lapsed between completion and receipt by BX.

Recommendation

We recommend the Executive for Business Support Services:

> **Recommendation 5:** Establish standards and procedures for the Personnel Security Program to ensure re-investigations, pre-screening, and follow-up on submitted investigations are completed timely.

Management Response

Business Support Services will develop and implement standard operating procedures for the Personnel Security Program to ensure re-investigations, pre-screening, and follow-up on submitted investigations are completed timely.

Target Completion Date: December 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 5. Lack of Controls over Adjudication Decisions

BX did not effectively manage the adjudication process. The condition occurred because BX lacked sufficient standard operating procedures and oversight of adjudication decisions. 5 C.F.R. Part 732.203 states when an agency makes an adjudicative decision under this part based on an OPM investigation, the agency must insure that the records used in making the decision are accurate, relevant, timely, and complete to the extent reasonably necessary to assure fairness to the individual in any determination. 5 C.F.R. 731.102(c) states agencies must also implement policies and maintain records demonstrating that they employ reasonable methods to ensure adherence to these OPM issuances. Without proper controls, there is limited assurance NARA has properly vetted employees in sensitive or covered positions.

The OIG reviewed BX Personnel Security's processes from receipt of the investigation report and related files to them notifying the program office of their adjudication decision and found multiple control issues in NARA's adjudication process:

- Favorable Adjudication of Questionable Cases – NARA favorably adjudicated 32 out of 33 "D Issue"[9] cases from FY 2015-2019, but we found at least five cases where the issues (e.g. arrests, debts, trustworthiness) associated with the case appeared disqualifying to the OIG. We also found other serious conduct issues, which were rated less serious by OPM. NARA's Deputy Chief Security Officer (DCSO) stated questionable cases are brought to their attention, however there was no evidence maintained in SCTS supporting any official higher than the PSO reviewed and made decisions on these cases. The DCSO also stated OPM provides oversight to the adjudication process and has accepted NARA's adjudication decisions for cases with serious conduct.
- Assignment of Staff to Cases – Cases are not formally assigned to Personnel Security staff, therefore, adjudicators can select which cases they want to work. BX does not have controls established for adjudicators to consider their independence in the cases, and recuse themselves or establish safeguards to prevent bias. While adjudicators stated they would recuse themselves from cases of friends or be free of bias in cases, the risk remains favoritism and bias could impact NARA's adjudications.
- Inconsistent Documentation in Files – BX lacked a standard form to document adjudication decisions. Some files included a detailed form with enough information for the OIG to understand the issues reviewed in the case, the location of the information supporting the decision, and the reasoning behind NARA's decision. Other files included brief handwritten notes without supporting information, and in some files, there was no documentation supporting adjudication decisions.

[9] Cases where issues are major, and the conduct or issue, standing alone, would be disqualifying.

- Timeliness of Adjudication Process – NARA did not always adjudicate cases timely. OPM guidance allowed 90 days to fully adjudicate cases. Of 620 adjudications reviewed, the OIG found about six percent took longer than the 90 days allowed.
    - Employee Response Times – Adjudicators experienced difficulty in obtaining additional information needed during investigations as some employees did not always respond timely. No procedures existed to outline response time expected from employees or when Personnel Security should elevate the employee's non-response to management. It should be noted NARA has taken action by encouraging staff to address any known issues prior to completion of investigation. However, some employees are still unprepared to provide requested documents and sufficiently address issues raised in their investigations.
    - Timeliness of Office Notification – Review of cases revealed delays in Personnel Security staff notifying offices of investigation results. No written procedures govern the timeframe, and emphasis is not always placed on performing these steps timely.

Recommendations

We recommend the Executive for Business Support Services:

Recommendation 6: Establish management oversight of the adjudication process, including more stringent review of serious adjudication issues with associated signoffs and documentation requirements.

Management Response

Business Support Services will develop and implement standard operating procedures for management oversight of the adjudication process. This will include a more stringent review of serious adjudication issues by the Director of Security Management. The Director will sign off on documentation.

Target Completion Date: December 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 7: Establish standards and review procedures for adjudication decisions and report the results of the review and monitoring activities.

Management Response

Business Support Service will establish and formalize reporting of the adjudication decisions and results to OPM. This report will use form INV FORM 79A-Report of Agency Adjudication Action on OPM Personnel Investigation.

Target Completion Date: August 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 8: Implement standard timeframes to complete adjudications.

Management Response

Business Support Services will develop and implement standard operating procedures that implements standard timelines to complete adjudications.

Target Completion Date: December 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 9: Implement standard response times from employees and follow-up procedures for Personnel Security.

Management Response

Business Support Services will develop and implement a standard operating procedure that follows Federal requirements for employee responses times, and will include notification and follow-up procedures with supervisors.

Target Completion Date: August 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 10: Implement controls to ensure adjudicator independence from cases reviewed.

Management Response

The Chief of Security, National Archives Building, is responsible for conducting the suitability adjudication of the Personnel Security staff for initial or for periodic investigations as they are scheduled. Effective June 5, 2020, the Personnel Security Staff will recuse themselves from adjudicating any investigations of any individuals they have close and continuing contact with and refer the case to the Director of Security Management for a determination of who will conduct the adjudication. This requirement will be incorporated into the update of NARA Directive 273, Administrative Procedure for Security Clearances.

Target Completion Date: Completed

OIG Analysis

We consider NARA's action responsive to our recommendation. This recommendation is closed and resolved.

Finding 6. Poor Data Quality in Security Clearance Tracking System

BX did not design and implement controls to ensure the integrity of its data in SCTS, NARA's system for background and security investigations. The condition occurred because BX lacked standard operating procedures and oversight of actions performed in SCTS. GAO's *Standards for Internal Control in the Federal Government* states management obtains relevant data from reliable internal and external sources in a timely manner based on the identified information requirements. Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management evaluates both internal and external sources of data for reliability. As a result, NARA has limited assurance data in SCTS is consistent, complete, and accurately recorded for background and security investigations.

BX has an Administration Guide for SCTS, but we found the document was not used and did not contain specific procedures for using the system. No procedures existed governing the specific processes of entering data in SCTS through all phases of the background investigation. Instead, NARA relied upon staff to know how, when, and what information to enter in SCTS.

We conducted several tests based on SCTS reports to assess the adequacy of NARA's controls over data in SCTS and found numerous issues including:

- Missing Employee Documentation – Two individuals listed as Active Employees (since 2013 and 2016, respectively), had no documentation in their case files. There is the risk NARA granted these two individuals clearances without proper vetting and clearances completed for individuals not related to NARA. We raised the concern to management, but they were unable to provide details regarding the clearances, but have since marked both individuals "Inactive" in SCTS.
- Missing Employees – At least one employee was not entered into SCTS. The PSO found the records of the employee addressed by the OIG, and scanned the information into SCTS. Another NARA employee told the OIG there were more employees missing from SCTS.
- Missing Contractors – Two of seven current NARA contractors in our sample had no entry in SCTS. Further, ITP staff **e**xpressed concern with contractor entries in SCTS and the impact of not knowing of all cleared contractors had on the program.
- Position Sensitivity Levels – There were variances in listed position sensitivity levels between SCTS and FPPS.
- Active and Inactive Employee Issues – We compared SCTS and FPPS and found a wide variance in active employees. The PSO stated SCTS may show more active employees than FPPS because Personnel Security is not consistently notified of employee departures who are not clearance holders. However, there was no evidence supporting proactive

action was taken by BX to obtain this information. The PSO relied upon internal communication documents, which did not always contain complete employee departure information. We found:

  - Specific employees listed as Inactive in SCTS while being Active in FPPS reports.
  - Specific employees listed as Active in SCTS but who did not appear in FPPS reports.
  - Double entered employees and contractors in SCTS.

- Missing information – There was missing information (investigation dates, sensitivity ratings, risk levels) within employee data in SCTS. Also, each employee profile in SCTS did not always contain the name of the personnel security specialist responsible for entry.
  - Also, four employees in FPPS were not given a sensitivity rating, despite two of the employees holding a top secret clearance.
- Outdated information – SCTS was not properly updated with current organizational codes for active employees. A manager requesting a report on clearances for their employees from SCTS might not receive all employees if an employee's organization code has not been updated.
- Field Control Issues – There was a lack of field controls and specific procedures on how to enter certain data in SCTS. Additionally, we found incorrect information included in fields (e.g. Office Codes in Position Series field).

Recommendations

We recommend the Executive for Business Support Services:

Recommendation 11: The Executive for Business Support Services ensure all active NARA employees and contractor files are scanned into Security Clearance Tracking System.

Management Response

Business Support Services will ensure that all active NARA employees and contractor files are scanned into SCTS and will provide certification of this review.

Target Completion Date: June 30, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 12: The Executive for Business Support Services establish standards and review procedures over the entry of information into Security Clearance Tracking System fields to ensure consistency and accuracy.

Management Response

Business Support Services will develop and implement procedures for the consistent and accurate entry of data into SCTS. In addition, the Personnel Security Officer will complete a 5% quality assurance review each fiscal year quarter to ensure that new files are uploaded and applicable fields are complete and accurate as required. This quality assurance will be added to the FY2021 Internal Control Program.

Target Completion Date: December 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 13: The Executive for Business Support Services ensure all Security Clearance Tracking System data fields are complete and accurate for active employees.

Management Response

The actions to complete Recommendations 11 and 12 will address this Recommendation.

Target Completion Date: June 30, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 14: The Executive for Business Support Services and Chief Human Capital Officer reconcile Federal Personnel Payroll System and Security Clearance Tracking System position sensitivity ratings to ensure the two systems accurately reflect the proper sensitivity rating.

Management Response

Business Support Services and Human Capital will reconcile Federal Personnel Payroll System and Security Clearance Tracking System position sensitivity determinations ratings to ensure the two systems mirror each other. This will be maintained by Human Capital who will provide Business Support Services a report per pay period reflecting position sensitivity changes. Security Management will update SCTS each pay period. For the first reconciliation, Security Management will provide Human Capital with an

exported report from SCTS of active individual's position sensitivity. Human Capital will conduct a crosswalk/reconcile utilizing FPPS data, review Alt OF-8/OF-8s and Position descriptions. Human Capital will update the position sensitivity designation records with the supervisors as well as coordinate with the human resources shared service provider for updating the Alt OF-8/OF-8 and position descriptions.

Target Completion Date: December 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 15: The Chief Human Capital Officer, in collaboration with Business Support Services, review discrepancies in position sensitivity ratings based on the reconciliation of Federal Personnel Payroll System and Security Clearance Tracking System data, and take action to correct any position descriptions that are not classified at the proper risk level for the position.

Management Response

After discrepancies are identified, Human Capital will work with the appropriate manager, and if required, document change via position designation tool, task the Human Capital shared services provider on updating position descriptions and Federal Personnel Payroll System data, and provide Business Support Services confirmed position sensitivity data.

Target Completion Date: December 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Appendix A – Acronyms

Acronym	Definition
BX	Security Management Division
C.F.R.	Code of Federal Regulations
DCSO	Deputy Chief Security Officer
FPPS	Federal Personnel Payroll System
FY	Fiscal Year
GAO	Government Accountability Office
ITP	Insider Threat Program
NARA	National Archives and Records Administration
OIG	Office of Inspector General
OPM	Office of Personnel Management
PSO	Personnel Security Officer
SCTS	Security Clearance Tracking System
SEAD	Security Executive Agent Directive
SF	Standard Form

Appendix B – Management Response

NATIONAL ARCHIVES

Date: June 16, 2020

To: James Springs, Inspector General

From: David S. Ferriero, Archivist of the United States

Subject: Action Plan to OIG Report 20-AUD-12, *Audit of NARA's Personnel Security and Suitability Program*

Thank you for the opportunity to provide comments on this final report. We appreciate your willingness to meet and clarify language in the report.

We concur with the 15 recommendations in this audit, and in response, the attachment provides a summary of our proposed actions. We are also providing documentation of actions taken to address Recommendation 10. As each recommendation is satisfied, we will provide documentation to your office. If you have questions about this action plan, please contact Kimm Richards at kimm.richards@nara.gov or by phone at 301-837-1668.

DAVID S. FERRIERO
Archivist of the United States

Attachment

NATIONAL ARCHIVES and RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Action Plan Response to OIG Report 20-AUD-12
Audit of NARA's Personnel Security and Suitability Program

Recommendation 1: We recommend the Executive for Business Support Services review, update, and implement revised NARA Directive 273, Administrative Procedures for Security Clearances, NARA Directive 273 Supplement, Supplement Administrative Procedures Related to Security Clearances and Applicant and Employee Rights, NARA Directive 275, Background and Identity Verification Process for Access Privileges, and NARA Directive 276, Employment or Service Suitability Determinations.

Planned Action: Business Support Services will review, update, and implement revised Directives: NARA Directive 273, Administrative Procedures for Security Clearances, NARA Directive 273 Supplement, Supplement Administrative Procedures Related to Security Clearances and Applicant and Employee Rights, NARA Directive 275, Background and Identity Verification Process for Access Privileges, and NARA Directive 276, Employment or Service Suitability Determinations. All standard operating procedures created in this action plan will be incorporated into the updated directives.

Target Completion Date: June 30, 2021

Recommendation 2: We recommend the Executive for Business Support Services ensure all Security Management Personnel Security staff is familiar with updated policies.

Planned Action: Business Support Services will ensure all Security Management Personnel Security staff are familiar with updated policies. Once the directives are updated and issued we will have staff read them and sign a statement that they understand and will follow the policy(s).

Target Completion Date: June 30, 2021

Recommendation 3: We recommend the Executive for Business Support Services implement standard formats for Human Capital notifications to Security Management Personnel Security.

Planned Action: Business Support Services will create a standardized form that will outline the required information Security Management Personnel Security needed from Human Capital.

Target Completion Date: December 31, 2020

Recommendation 4: We recommend the Executive for Business Support Services develop and implement standard operating procedures for: position risk designations;

access requirements for federal employees; background investigations; suitability and security clearance determinations; granting, suspending, or revoking security clearances; and any other aspects of the Personnel Security Program that Management determines requires standard operating procedures.

Planned Action: Business Support Services will develop and implement standard operating procedures for: position risk designations; access requirements for federal employees; background investigations; suitability and security clearance determinations; granting, suspending, or revoking security clearances.

Target Completion Date: December 31, 2020

Recommendation 5: We recommend the Executive for Business Support Services establish standards and procedures for the Personnel Security Program to ensure re-investigations, pre-screening, and follow-up on submitted investigations are completed timely.

Planned Action: Business Support Services will develop and implement standard operating procedures for the Personnel Security Program to ensure re-investigations, pre-screening, and follow-up on submitted investigations are completed timely.

Target Completion Date: December 31, 2020

Recommendation 6: We recommend the Executive for Business Support Services establish management oversight of the adjudication process, including more stringent review of serious adjudication issues with associated signoffs and documentation requirements.

Planned Action: Business Support Services will develop and implement standard operating procedures for management oversight of the adjudication process. This will include a more stringent review of serious adjudication issues by the Director of Security Management. The Director will sign off on documentation.

Target Completion Date: December 31, 2020

Recommendation 7: We recommend the Executive for Business Support Services establish standards and review procedures for adjudication decisions and report the results of the review and monitoring activities.

Planned Action: Business Support Service will establish and formalize reporting of the adjudication decisions and results to OPM. This report will use form INV FORM 79A-Report of Agency Adjudication Action on OPM Personnel Investigation.

Target Completion Date: August 31, 2020

Recommendation 8: We recommend the Executive for Business Support Services implement standard timeframes to complete adjudications.

Planned Action: Business Support Services will develop and implement standard operating procedures that implements standard timelines to complete adjudications.

Target Completion Date: December 31, 2020

Recommendation 9: We recommend the Executive for Business Support Services implement standard response times from employees and follow-up procedures for Personnel Security.

Planned Action: Business Support Services will develop and implement a standard operating procedure that follows Federal requirements for employee responses times, and will include notification and follow-up procedures with supervisors.

Target Completion Date: August 31, 2020

Recommendation 10: We recommend the Executive for Business Support Services implement controls to ensure adjudicator independence from cases reviewed.

Actions Taken: The Chief of Security, National Archives Building, is responsible for conducting the suitability adjudication of the Personnel Security staff for initial or for periodic investigations as they are scheduled. Effective June 5, 2020, the Personnel Security Staff will recuse themselves from adjudicating any investigations of any individuals they have close and continuing contact with and refer the case to the Director of Security Management for a determination of who will conduct the adjudication. This requirement will be incorporated into the update of NARA Directive 273, Administrative Procedure for Security Clearances.

Target Completion Date: Completed

Recommendation 11: We recommend the Executive for Business Support Services ensure all active NARA employees and contractor files are scanned into Security Clearance Tracking System.

Planned Action: Business Support Services will ensure that all active NARA employees and contractor files are scanned into SCTS and will provide certification of this review.

Target Completion Date: June 30, 2021

Recommendation 12: We recommend the Executive for Business Support Services establish standards and review procedures over the entry of information into Security Clearance Tracking System fields to ensure consistency and accuracy.

Planned Action: Business Support Services will develop and implement procedures for the consistent and accurate entry of data into SCTS. In addition, the Personnel Security Officer will complete a 5% quality assurance review each fiscal year quarter to ensure that new files are uploaded and applicable fields are complete and accurate as required. This quality assurance will be added to the FY2021 Internal Control Program.

Target Completion Date: December 31, 2020

Recommendation 13: We recommend the Executive for Business Support Services ensure all Security Clearance Tracking System data fields are complete and accurate for active employees.

Planned Action: The actions to complete Recommendations 11 and 12 will address this Recommendation.

Target Completion Date: June 30, 2021

Recommendation 14: We recommend the Executive for Business Support Services and the Chief Human Capital Officer reconcile Federal Personnel Payroll System and Security Clearance Tracking System position sensitivity ratings to ensure the two systems accurately reflect the proper sensitivity rating.

Planned Action: Business Support Services and Human Capital will reconcile Federal Personnel Payroll System and Security Clearance Tracking System position sensitivity determinations ratings to ensure the two systems mirror each other. This will be maintained by Human Capital who will provide Business Support Services a report per pay period reflecting position sensitivity changes. Security Management will update SCTS each pay period. For the first reconciliation, Security Management will provide Human Capital with an exported report from SCTS of active individual's position sensitivity. Human Capital will conduct a crosswalk/reconcile utilizing FPPS data, review Alt OF-8/OF-8s and Position descriptions. Human Capital will update the position sensitivity designation records with the supervisors as well as coordinate with the human resources shared service provider for updating the Alt OF-8/OF-8 and position descriptions.

Target Completion Date: December 31, 2020

Recommendation 15: We recommend the Chief Human Capital Officer, in collaboration with Business Support Services, review discrepancies in position sensitivity

ratings based on the reconciliation of Federal Personnel Payroll System and Security Clearance Tracking System data, and take action to correct any position descriptions that are not classified at the proper risk level for the position.

Planned Action: After discrepancies are identified, Human Capital will work with the appropriate manager, and if required, document change via position designation tool, task the Human Capital shared services provider on updating position descriptions and Federal Personnel Payroll System data, and provide Business Support Services confirmed position sensitivity data.

Target Completion Date: December 31, 2020

Appendix C – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief of Management and Administration
Executive for Business Support Services
Accountability
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee

OIG Hotline

To report fraud, waste, or abuse, please contact us:

Electronically: OIG Hotline Referral Form

Telephone:
301-837-3500 (Washington, D.C. Metro Area)
1-800-786-2551 (toll-free and outside the Washington, D.C. metro area)

Mail:
IG Hotline
NARA
P.O. Box 1821
Hyattsville, MD 20788-0821