NATIONAL ARCHIVES | Inspector General

February 4, 2026

TO: Valorie Findlater
Chief of Management and Administration

FROM: William Brown
Acting Inspector General

SUBJECT: *Audit of NARA's Security Management Program*
OIG Audit Report No. 26-AUD-02

The Office of Inspector General (OIG) contracted with Sikich CPA LLC (Sikich) to conduct an independent performance audit of NARA's Security Management Program. The objective of this audit was to evaluate the efficiency and effectiveness of NARA's Security Management program, including whether guard contract vendor payments made by NARA at selected Presidential Libraries were reasonable and properly supported by services provided, in accordance with contractual provisions. Sikich is responsible for the attached auditor's report dated February 4, 2026 and the conclusions expressed in the report. The findings and conclusions presented in the report are the responsibility of Sikich. The OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with Generally Accepted Government Audit Standards.

The report contains seven recommendations made to strengthen NARA's security management program and strengthen oversight of funds used for contracted security guards. Given the significant issues identified during the course of this audit, the OIG plans to conduct further oversight work into security force contracts to further assist NARA with strengthening controls. The OIG looks forward to the continued cooperation with NARA during our oversight work in this important area.

Please provide planned corrective actions and expected dates to complete the actions for each of the recommendations within 30 days of the date of this report. As with all OIG products, we determine what information is publicly posted on our website from the published report. Consistent with our responsibility under the Inspector General Act of 1978, as amended, we may provide copies of our report to congressional committees with oversight responsibility for NARA. We appreciate the cooperation and assistance NARA extended to us during this audit. Please contact me with any questions.

SIKICH®

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
SECURITY MANAGEMENT PROGRAM
PERFORMANCE AUDIT

SUBMITTED TO THE
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

PERFORMANCE AUDIT REPORT

FEBRUARY 4, 2026

TABLE OF CONTENTS

333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

SIKICH.COM

February 4, 2026

William Brown
Acting Inspector General
Office of Inspector General
National Archives and Records Administration

Dear Mr. Brown,

Sikich CPA LLC (Sikich) is pleased to submit the attached report detailing the results of our performance audit of the National Archives and Records Administration's (NARA's) Security Management program, conducted under contract number 88310323A-00012, order 88310324F00249.

The objective of this performance audit was to evaluate the efficiency and effectiveness of NARA's Security Management program, including whether guard contract vendor payments made by NARA at selected Presidential Libraries were reasonable and properly supported by services provided, in accordance with contractual provisions. This report is a public version of a sensitive report issued in January 2026. This report omits specific details regarding security measures, threats, and vulnerabilities, which could pose unintended security risks. Although the information provided in this report is more limited, the report addresses the same objectives as the report containing sensitive information and uses the same methodology.

We conducted the audit fieldwork in Alexandria, Virginia; Atlanta, Georgia; Kansas City, Missouri; Riverside, California; Simi Valley, California; Yorba Linda, California; St. Louis, Missouri; College Park, Maryland; Washington, DC; and remotely from September 2024 through November 2025. We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, as issued by the Comptroller General of the United States (2018 Revision, Technical Update April 2021). 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 objectives. We describe our objective, scope, and methodology further in **Appendix A: Objective, Scope, and Methodology.**

We would like to thank all the NARA and contractor personnel with whom we met, or who provided information, for their cooperation and assistance.

Sincerely,

Sikich CPA LLC

EXECUTIVE SUMMARY

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) engaged Sikich CPA LLC (Sikich) to conduct a performance audit to evaluate the efficiency and effectiveness of NARA's Security Management program. This report is a public version of a sensitive report issued in January 2026. This report omits specific details regarding security measures, threats, and vulnerabilities, which could pose unintended security risks. Although the information provided in this report is more limited, the report addresses the same objectives as the report containing sensitive information and uses the same methodology.

Performance Audit of NARA'S Security Management Program	
Why Did We Conduct this Audit? NARA's mission is to preserve, protect, and share the historical records of the United States to promote public inquiry and federal government accountability. NARA's Security Management Division is responsible for preventing and responding to incidents at NARA's 40 facilities across 17 states and Washington, DC. This audit's objective was to evaluate the efficiency and effectiveness of NARA's Security Management program, including whether guard contract vendor payments made by NARA at selected Presidential Libraries were reasonable and properly supported. To address this objective, we reviewed relevant policies, procedures, and guidance, including the Interagency Security Committee's (ISC) *Risk Management Process* (RMP) standards, which set the physical security standards for federal facilities. We visited 15 NARA facilities including Research facilities, Federal Record Centers (FRCs), and Presidential Libraries to observe and discuss physical security measures, facility security assessments, and incident reporting. We also examined incident reports for the selected facilities to determine the extent of reported security concerns and to assess NARA's process for collecting incident data. Additionally, we sampled guard contracts, timesheets, and guard status reports for selected Presidential Libraries and examined documentation to determine whether invoices were properly supported prior to payment.	**What Did We Find?** We found that NARA has generally complied with ISC standards, policies, and recommendations. However, NARA has opportunities to better align security practices with ISC standards and improve security incident data controls. Specifically, we found certain NARA Facility Security Level determination scores were inaccurate or inconsistent, and identified several weaknesses related to NARA's process for assigning threat, vulnerability, and consequence scores. In particular, NARA did not provide written justification for the scores. We also found that NARA did not consistently obtain, track, or analyze security incident information in a centralized database. NARA also did not document its consideration of reported security incidents when assessing risk. In addition, we found that NARA could not provide sufficient documentation in support of the invoices associated with security guard contracts at three selected Presidential Libraries. As a result, we identified total questioned costs of $158,880.29. We also found that NARA approved $9,093.65 unallowable supply and material charges. **What Did We Recommend?** We are making seven recommendations to strengthen NARA's security management program and strengthen oversight of funds used for contracted security guards.

SUMMARY OF RECOMMENDATIONS

Number	Recommendation	Responsible Office
1	Update the Facility Security Risk Management Program Internal Operating Procedure (IOP) to include. • Additional guidance on how to implement the Interagency Security Committee's (ISC) Standard's Facility Security Level (FSL) criteria. • A process for documenting the Chief, Physical Security's approval of the FSL. • A requirement for supporting documentation and justification for each assigned score, including source references or observed conditions that could impact certain criteria. • A requirement for documented justifications for any deviations from the Design Basis Threat (DBT) baseline scores identified by ISC. • A requirement that security incident data be reviewed, analyzed, and attached as part of the Facility Security Assessment (FSA) process.	Executive for Business Support Services in coordination with the Security Management Division (BX) Director
2	Develop and implement policies and procedures for centrally obtaining, tracking, and analyzing security incident reports agency-wide.	Executive for Business Support Services in coordination with the BX Director
3	Develop and implement standard operating procedures (SOPs) that instruct CORs on the invoice approval process, to include a requirement that CORs document their reconciliation of invoices with detailed timesheets before security guard contract invoices are paid.	Executive for Business Support Services in coordination with the Acquisitions Division (BZ) Director and the Executive for Presidential Libraries
4	Recover or otherwise resolve the $158,880.29 in questioned costs from security guard vendors as a result of insufficient documentation.	Executive for Business Support Services in coordination with the BZ Director and the Executive for Presidential Libraries
5	Provide training on the new documentation requirements to any COR responsible for security guard contracts.	Executive for Business Support Services in coordination with the BZ Director
6	Recover or otherwise resolve the $9,093.65 in questioned costs from the security guard vendor at the Truman Presidential Library related to unallowable supply and material charges.	Executive for Business Support Services in coordination with the BZ Director and the Executive for Presidential Libraries
7	Provide specific guidance to CORs responsible for security guard contracts or, as appropriate, issue a contract modification which further clarifies the allowable uses for the "Additional Services" Contract Line Item Numbers (CLINs), and processes required to use available funds for other purposes.	Executive for Business Support Services in coordination with the BZ Director

BACKGROUND

NARA is a distinct agency within the Executive Branch of the United States government responsible for preserving, protecting, and providing access to the records of our federal government. NARA's mission is to preserve, protect, and share the historical records of the federal government to promote public inquiry and federal government accountability. As of 2025, NARA has 40 facilities in 17 states, plus the District of Columbia. These facilities include

Research Facilities, FRCs, and Presidential Libraries. Across these facilities, NARA maintains approximately 91 million photographs, aerial images, maps, charts, and architectural/engineering drawings; 13.5 billion pieces of paper; and more than 725,000 artifacts, among other things. In 2024 NARA had more than 2.1 million visitors to its museums and more than 45,000 visitors to its research rooms.

NARA's Executive for Business Support Services serves as NARA's Chief Security Officer and provides executive guidance to managers of NARA's information, personnel, safety, and physical security programs. NARA's Security Management Division (BX) is responsible for developing and administering NARA internal security policies, procedures and guidelines; implementing ISC requirements, including conducting facility security assessments; and for providing management and oversight of security guard contracts.

The Chief Security Officer delegates direct responsibility for facility security to other NARA offices, dependent on the purpose of the facility:

- Research Services – responsible for establishing physical and management controls associated with the storage, arrangement, and security of accessioned and donated records and the space housing them.
- The Office of Presidential Libraries – responsible for establishing physical and management controls associated with the storage, arrangement, and security of presidential records and the space housing them.
- Agency Services – responsible for overseeing NARA's program for classifying, safeguarding and declassifying national security information in both Government and industry.

In addition, certain NARA facilities are owned or leased by the General Services Administration (GSA). For these facilities, the Federal Protective Service (FPS) is the primary security agency, responsible for conducting facility security assessments and providing guard services or contracts. However, NARA's Chief Security Officer retains decision-making authority related to the security countermeasures FPS recommends.

For the purposes of this report, we selected a nonrepresentative sample of 15 NARA facilities based on location, facility type, FSL, and facility size, among other things. Of these 15 facilities, nine were owned or leased from commercial entities by NARA, while six were owned or leased by GSA.

The Interagency Security Committee (ISC) Risk Management Process (RMP)

The ISC—housed within the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency—is responsible for developing federal security policies and standards to enhance the quality and effectiveness of security in, and protection of, civilian federal facilities.[1] The ISC RMP standard and associated appendices define the criteria and processes to be used to determine the minimum physical security requirements and associated countermeasures for federal facilities based on the security level of the facility.[2] Federal regulations require nonmilitary federal facilities to meet the physical security standards as identified by the ISC.[3] Executive Order 12977 also directs the ISC to oversee the

[1] The ISC is chaired by an official from the Cybersecurity and Infrastructure Security Agency via a delegation from the Secretary of Homeland Security.
[2] The ISC defines facility security levels on a scale from Level I (lowest risk) to Level V (highest risk). The facility security level is determined by the facility security committees after an assessment of security criteria.
[3] 41 CFR § 102-81.25.

implementation of appropriate countermeasures in federal facilities.

The ISC RMP standard includes the following requirements:

- *Facility Security Level (FSL) Determination:* The FSL determination is the first step in the RMP Standard and must be performed prior to each risk assessment. FSL determinations range from Level I (lowest risk) to Level V (highest risk). The FSL is based on an analysis of six security-related facility factors, five of which are required. Figure 1. shows the FSL factors and scoring criteria.

Figure 1. Facility Security Level Determination Matrix

Factor	Points				Score
	1	2	3	4	
Mission Criticality	MINIMUM	LOW	MEDIUM	HIGH	
Symbolism	MINIMUM	LOW	MEDIUM	HIGH	
Facility Population	<100	101-250	251-750	>750*	
Facility Size	<10,000 Sq. ft.	10,001-100,000 sq. ft.	100,001 – 250,000 sq. ft.	>250,000 sq. ft	
Threat to Tenant Agency	MINIMUM	LOW	MEDIUM	HIGH	
					Sum of Above
Facility Security Level	I: 5-7 Points	II: 8-12 Points	III: 13-17 Points	IV: 18-20 Points	**Preliminary FSL**
Intangible Adjustment					**+/- 1 FSL**
					Final FSL
* Facilities with a child-care center (CCC) receives a facility population value of "high."					

Source: Interagency Security Committee Risk Management Process Standard, 2024

The five required factors are: mission criticality, symbolism, facility population, facility size, and threat to tenant agencies.[4] Assessors must evaluate and assign scores to these five FSL factors to calculate a preliminary FSL. As needed, assessors may also consider a sixth factor— the intangible factor—to adjust the FSL one level up or down based on other characteristics unique to the facility.[5] Each FSL corresponds to a level of risk for the facility, which directly relates to a baseline level of protection, or the specific countermeasures required to mitigate that level of risk.

[4] According to the RMP standard, the mission criticality score is based on criticality of the missions carried out by federal tenants in the facility (not by the tenant agencies overall). The symbolism score is based on external appearances or well-known operations within the facility that indicate it is a U.S. Government facility, as well as the potential negative psychological impact of an undesirable event occurring at the facility. The facility population score is based on the peak total number of personnel in government space, including employees, on-site contract employees, and visitors. The facility size score is based on the square footage of all federally occupied space in the facility. Lastly, the threat to tenant agencies score is based on the nature of federal tenant's contact with the public and the mission at the facility; past or current credible threats to the federal tenants at the facility (including indirect threats to federal tenants caused by threatening nonfederal tenants); and crime statistics.

[5] For example, the RMP standard states that agencies may justify reducing the preliminary FSL due to factors such as a short duration of occupancy at a facility, which may reduce the value of the facility in terms of investment or mission. Agencies may justify increasing the preliminary FSL due to factors such as the potential for cascading effects or downstream impacts on interdependent infrastructure, or costs associated with the reconstitution of the facility.

- *Facility Security Assessments (FSA)*: The FSA is the process and final product documenting an evaluation of the security-related risks to a facility. The process analyzes potential threats, vulnerabilities, and estimated consequences using a variety of sources and information and the FSA provides documentation of the ISC's required recurring risk assessments. The ISC RMP standard does not require agencies to use a specific risk assessment methodology, but does require that the methodology be defensible, credible, and assess the threat, vulnerability, and consequence to specific undesirable events.
    - **Threat:** The intention and capability of an adversary to initiate an undesirable event.
    - **Vulnerability:** A weakness in the design or operation of a facility that an adversary can exploit.
    - **Consequence:** The level, duration, and nature of the loss resulting from an undesirable event.

    The ISC RMP appendices identify 33 undesirable events (UEs) that agency personnel must consider in their risk assessments, as well as the baseline threat ratings associated with each UE. The appendices also identify specific security countermeasures required for certain identified risk levels. To be considered defensible, the ISC requires agencies to provide sufficient justification for deviating from the baseline threat ratings or levels of protection.

    To carry out this requirement in NARA-owned or leased facilities, NARA has developed a risk assessment methodology referred to as the Risk Management Program Tool (RMPT). As discussed previously, for those NARA facilities that are GSA-owned or leased, FPS conducts the FSA. FPS uses a different automated Threat Assessment tool. While these assessments result in recommended security measures for NARA facilities, the FPS risk assessment process and results were outside the scope of this audit.

AUDIT RESULTS

We found that NARA has generally complied with the requirements of ISC standards, policies, and recommendations, but identified several areas for improvement. Below, we provide detailed information regarding findings for NARA to better align security practices with ISC standards and improve security incident data controls. In addition, we found that NARA could not provide sufficient supporting documentation for security guard invoices at selected Presidential Libraries.

Finding 1: Opportunities to Better Align Security Practices with ISC Standards

For the nine facilities where NARA completed the FSA, we found certain NARA FSL determination scores were inaccurate or inconsistent, and identified several weaknesses related to NARA's process for assigning threat, vulnerability, and consequence scores using the RMPT. Specifically:

- *Inaccurate Facility Size score*: NARA's 2023 FSL determination for the Atlanta FRC resulted in a score of "2" for that facility, which has a size of 352,064 square feet. However, the ISC RMP requires facilities with a size greater than 250,000 square feet to be assigned a score of "4".
- *Inconsistent Rationale for Threat to Tenant Agencies score*: NARA assigned Threat to Tenant Agencies scores of "3" for both the Jimmy Carter Presidential Library and Atlanta

Archives with the rationale statement that they are "located in a high-crime area," which is supported by the Crime Reports provided in the FSAs. However, NARA assigned the Harry Truman Presidential Library and Riverside FRC Threat to Tenant Agencies scores of "3" with the rationale statement that they are "located in a moderate crime area," also supported by the Crime Reports provided within the FSAs.

In addition, we found weaknesses related to NARA's process for assigning threat, vulnerability, and consequence scores. The ISC RMP Standard provides baseline threat scores and scoring guidelines for assigning vulnerability and consequence.[6] While the ISC allows for deviations from the baseline scores, it requires agencies to provide sufficient justification, using historical security incident information, current crime statistics, or actionable intelligence. Justifications for any deviations should summarize the identified risk, risk mitigation measures or alternative countermeasures, and the achievable level of protection the alternative measure will provide. Similarly, the ISC appendices provide event scenarios for each identified UE to assist agencies in determining vulnerability and consequence scores. Vulnerability scores should reflect the ability of existing countermeasures to resist or overcome the event scenario, while consequence scores should reflect the potential effect of a successful UE. However, we found that NARA consistently deviated from baseline threat scores without justification and did not sufficiently consider vulnerability and consequence. Specifically:

- *Threat*: For the FSAs we reviewed, NARA consistently deviated from the threat levels established by ISC standards. The FSAs did not document justification for these specific deviations. As an example, NARA consistently rated certain UEs as "high" or "very high" risk, even though the ISC identified them as either "minimum" or "low" risk.
- *Vulnerability:* NARA also disproportionately emphasized three UEs when assigning vulnerability scores. In 8 of the 9 FSAs we reviewed, NARA assigned the same vulnerability score to all but the three emphasized UEs.[7] The FSAs did not document justifications for these scores. In addition, we noted that vulnerability scores did not always reflect the information contained in the FSA. For example, in two FSAs we reviewed, NARA assigned the lowest possible vulnerability score to UE categories that were specifically related to security deficiencies noted in the same report.
- *Consequence*: All FSAs reviewed applied a single consequence score for all 33 UEs, without considering the unique potential consequence of each UE.
- *Security Incident Reports*: NARA FSAs did not clearly indicate how facility-specific security incident information is considered when assessing risks and determining the facility's necessary Level of Protection. Although a checklist attached to the FSA indicated that the security specialist reviewed facility security incidents, no additional evidence was included within FSA documentation demonstrating how incidents factored into the risk assessment process. As an example, at one location, multiple security incidents were documented as "Security Violations" during Fiscal Years (FYs) 2022 through 2024. However, the FSA

[6] ISC, *The Risk Management Process: Appendix A: Design Basis Threat (DBT) Report*, Section 4.3 Risk Assessments, notes that agencies must use the DBT as a baseline for estimating threat, vulnerability, and consequence for each UE in their assessment process. Specifically, agencies are expected to: (1) Document and justify any deviation from the DBT using current crime statistics or actionable intelligence; (2) Provide detailed rational for any modifications to DBT scenarios used in scoring; (3) Tailor consequence estimates based on the potential impact of a successful UE; (4) Evaluate vulnerability by considering how well existing protective measures would resist the DBT scenario. This section also notes that agencies may adjust baseline threat levels using facility or location-specific intelligence such as crime statistics, but any modifications must be fully documented.
[7] The 9th FSA we reviewed included other vulnerability scores for 5 UEs.

conducted in 2024 did not reference these incidents in its risk analysis, and there is no evidence that the reported incidents affected the facility's threat or vulnerability scores.

We found that the issues we identified were caused by deficiencies in NARA's *Facility Security Risk Management Process Internal Operating Procedures* (IOP). Specifically, while NARA's IOP references the FSL determination requirements in the ISC standard and directs assessors to complete the FSL determination based on the ISC standard and the facility-specific data gathered through the assessment, it does not provide any further guidance on FSL determination. As a result, the IOP does not include sufficient detail to ensure BX Security Specialists are consistently assigning FSLs across all NARA facilities. In addition, although the IOP requires the Chief, Physical Security to review and approve each FSL determination, the FSAs in our performance audit did not include any indication of this approval, in part because the IOP does not explicitly identify how this requirement is to be documented.

We also determined that NARA's IOP does not fully align with ISC's requirements for assessing threat, vulnerability, and consequence, causing the deficiencies in the risk assessments we reviewed. In particular, the IOP does not require assessors to tailor consequence scores to the potential impact of specific UEs. Additionally, NARA's IOP requires assessors to document justification for any adjustment to threat, vulnerability, and consequence scores calculated using RMPT. However, the IOP does not require documented support for deviations from the baseline threat scores provided by the ISC.

The IOP also includes a requirement for assessors to consider facility-specific information; however, it does not specifically require security specialists to consider actual security incidents in FSAs or document how these incidents influenced the assigned threat, vulnerability, or consequence scores.

Without updating the IOP to address these deficiencies, NARA risks inaccurate, inconsistent, or unsupported results from its facility security assessment process. Inaccurate or inconsistent FSL factor scores compromise the integrity of NARA's risk management process. FSL scoring is the first step in determining the level of protection equal to the level of risk at a site-specific location. Inaccurate, inconsistent, or unsupported FSL scores may result in an inaccurate assessment of a facility's security posture, potentially leading to wasted resources or unmitigated risks.

Inaccurate or unsupported evaluation of threat, vulnerability, and consequences for each undesirable event increases the risk that NARA facilities are not properly protected relative to known threats. Additionally, without thoroughly considering and incorporating security incident data into FSAs, NARA may not fully account for threat conditions or existing vulnerabilities. This may result in inaccurate evaluation of risk and protective measures at facilities.

Therefore, we recommend NARA's Executive for Business Support Services coordinate with the BX Director:

Recommendation 1: Update the Facility Security Risk Management Program IOP to include:

a. Additional guidance on how to implement the ISC Standard's FSL criteria.

b. A process for documenting the approval of the FSL by the Chief, Physical Security's approval of the FSL.

c. A requirement for supporting documentation and justification for each assigned score, including source references or observed conditions that could impact certain criteria.

d. A requirement for documented justifications for any deviations from the DBT baseline scores identified by ISC.

e. A requirement that security incident data be reviewed, analyzed, and attached as part of the FSA process.

Finding 2: Opportunities to Improve NARA's Security Incident Data

We found that BX personnel did not consistently obtain, track, or analyze security incident information in a centralized database. We requested security incident data from BX and the 13 field facilities we selected for review.[8] Of the 15 selected facilities, we received incident reports for 12 facilities.[9] This included logs that are maintained directly by BX for the National Archives I and II facilities.

As of July 2025, when a significant incident occurs at a facility, officers from that facility complete a hard copy of the incident report using NA Form 6037, *Offense/Incident and Investigation Report*. Each facility maintains the paper incident reports in a locally stored binder. In some instances, the facility may report an incident to BX by calling the BX security console located at NARA Archives II. The BX security console maintains a log in a spreadsheet containing both its own incidents and any incident calls from other facilities. According to BX officials, the NARA Archives II call center log serves as the division's primary document for capturing and tracking incident data nationally across NARA facilities.

BX personnel provided us with the security incident spreadsheet for FYs 2022 through 2024. The spreadsheet includes 23 incidents for NARA facilities other than NARA Archives II, including those within the scope of this audit. However, when we compared incident reports from sampled NARA facilities to the NARA Archives II call center log, we noted that it did not include any of the 172 security-related incident reports we obtained from the selected facilities. Additionally, as reported in finding 1, the FSAs we reviewed did not indicate how the assessor factored these security incident reports into NARA's FSL determination or assessment of threat or vulnerability.

We found this occurred because NARA has not developed a process or procedures to centrally obtain, track, or analyze security incidents nationally. While NARA's *IOP,* Appendix A, *Architecture and Design Security Standards for Presidential Libraries,* and Appendix B, *Architecture and Design Security Standards for Archives and Records Centers*, require that any concern of a significant security risk must be reported immediately to BX, the IOP does not define what constitutes a significant security risk and does not specify how BX is to track or analyze reported incidents.

According to the Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government,*[10] management should design policies, procedures, and mechanisms that carry out management's directives, define responsibilities, assign roles, delegate authority, and align with risk assessments to ensure an effective system of internal control. Further,

[8] BX is responsible for the security incidents that occur at National Archives I, in Washington, DC, and National Archives II, in College Park, MD.
[9] Three facilities – Lee's Summit FRC, Kansas City FRC, and Kansas City Archives – did not provide any incident reports, because they stated that no incidents occurred during the scope of our performance audit.
[10] GAO, *Standards for Internal Control in the Federal Government*, Sept. 2014.

management should use quality information to achieve objectives by identifying information requirements, ensuring data comes from reliable sources, and processing it into usable form. Developing a process to obtain, track, and analyze security incidents agency-wide would provide NARA greater insight to evolving threats or risks faced by facilities across the agency.

Therefore, we recommend NARA's Executive for Business Support Services coordinate with the Security Management Division (BX) Director:

> ***Recommendation 2:*** Develop and implement policies and procedures for centrally obtaining, tracking, and analyzing security incident reports agency wide.

Finding 3: NARA Could Not Provide Sufficient Invoice Documentation Related to Security Guard Contracts at Selected Presidential Libraries

For the Carter, Reagan, and Truman Presidential Libraries, we found that the documentation provided was not sufficiently detailed to allow for full reconciliation of the hours and fees on the invoices to the supporting documentation. We selected a random sample of 12 months and the associated invoices from each of the three selected Presidential Libraries and requested support to determine whether guard contract vendor payments were reasonable and properly supported by services provided, in accordance with contractual provisions. Each of the guard contracts we reviewed included a fixed-price amount for regular security guard services and hourly rates for additional services, such as special events. The fixed-price amount was established for the contract's period of performance, by guard position (supervisory/non-supervisory) and divided evenly by month. The individual contracts generally established expected daily and weekly coverage amounts for their respective facility, according to the guard's position/role and relevant post number.

All three selected Presidential Libraries utilized similar security guard contract language regarding the documentation required for the vendors' monthly status reports. Specifically, the contract provisions read:

> *…J. Purpose: To provide a summary of the previous month's activities and to identify any issues or concerns, and to identify upcoming training, events, schedules, etc.*
>
> *…L. PREPARATION INFORMATION*
> 1. *The report must be in vendor format.*
> 2. *As a minimum, the report must contain the following:*
>   a. *Status of the vendor activities against plans as an indication of performance;*
>   b. *Identification of significant issues, problems, or concerns related to performance or administration;*
>   c. *Statistics on the suitability and stability of the work force, i.e., absenteeism, turnover rates, and behavioral infractions;*
>   d. *Training accomplished during the month; and*
>   e. *Summary of incidents and injuries during the month.*
>   f. *Upcoming training, events, concerns, schedule changes, expiring credentials, etc.*
> 3. *Provide analysis of the data from the vendor's records of time of arrival and departure with the manpower requirements reported in the following formats: (1) period to date basis with the reporting period being the first through the last day*

of the previous month, and (2) a cumulative basis. The following information must be provided in each format:

a. Total hours expended by fiscal year for the reporting period;

b. Total hours expended by [Contract Line Item Number (CLIN)] for the reporting period;

c. Total hours expended by skill category within the specified CLIN for the reporting period; and

d. Daily hours logged by individual personnel (by name) within the specified skill category and CLIN for the reporting period.

4. *Provide a summary of the monthly prices by CLIN and task order total, on a monthly and cumulative basis.*

Carter Presidential Library

For most of the selected months, NARA provided a copy of an invoice, as well as the associated monthly summary reports and sign-in sheets that the Carter Presidential Library security guard contractor submitted as part of its required monthly deliverables. NARA did not provide all requested information for our selection. Specifically, NARA did not provide:

- 6 of the 12 selected invoices.
- 2 of the 12 monthly status reports.
- 1 of the 12 monthly sign-in sheets.

Invoices

For four of the six selected invoices which NARA provided, we determined that the amounts charged on the invoices matched the respective contract amounts. However, for the remaining two invoices, four of the line-item charges did not match available contract documentation, resulting in total discrepancies of as much as $2,758.

Monthly Status Reports and Sign-In Sheets

The monthly status reports are brief, one- to three-page documents. Although attachments are noted, NARA did not provide them. For eight of the selected months, NARA provided sign-in sheets that used NA Form 6019, *Contractor Guard Duty Register.* For the other three months, contactor sign-ins were captured on NA Form 6014, *Contractors: Record of Time of Arrival and Departure from Building.* None of these documents include a detailed list of guard employees and their position titles, a record of the total hours expended within each CLIN for the month, a list of the additional services provided in a given month, or reliable information regarding guard posts.

Although the sign-in sheets provide some insight to daily hours, we determined they were not reliable for the purposes of reconciling the invoiced amounts. Specifically, we found that 6 of 11 sign-in sheets did not include all days of the selected month, and in 2 instances, there was only a single entry for a given day. In addition, the sign-in sheets that used NA Form 6014 also appear to include entries from various other contractor organizations and do not indicate the post to which each guard was assigned.

During the scope period, the Carter Presidential Library had two active contracts, with numerous associated modifications. Both contracts include provision 4.5.1 "Ensure all posts are manned as required by the task order (See Attachment 2, Carter Library Security Post Hours)"

- The first contract (GS-07F-0168T) Attachment 2 included a supervisor position and three posts, totaling 432 hours of service per week.

- The second contract (GS-07F-0512V) Attachment 2 included a supervisor position and four posts, totaling 350 hours per week.

We selected a haphazard sample of 1 day from each of the 11 provided sign-in sheets and found:

- The number of guards signing in for the selected days ranged from 2 through 8.
- For 8 of the 11 days, the departure time was not noted for all guards.
- For 8 of 11 sign-in sheets that use NA Form 6019, which includes a field for the guards to identify their assigned post, we found:
  - 3 of 8 had at least one post entry left blank on the selected day.
  - 5 of 8 contained at least 1 illegible post number for the selected day.
  - None indicated that any guards were assigned to Post 4 for the selected day.
  - 6 of 8 did not indicate that any guard was assigned to Post 3 for the selected day.
  - 3 of 8 did not indicate that any guard was assigned to Post 2 for the selected day.

The lack of documentation we identified can be largely attributed to known issues with one of the Carter Presidential Library's security guard contractors. For the security guard contractor in place for the majority of our scope period (from May 2022 through September 2024), NARA documented numerous problems with contract performance. According to NARA officials, these problems ultimately resulted in the termination of the contract by not exercising Option Year II. The cited concerns included:

- Staffing and turnover issues, resulting in an inability to cover the required shifts with appropriately qualified personnel.
- Operational failures and negligence, including lapses in communication and inappropriate behavior by guards.
- Supervision and training issues, resulting in unmanned posts and guards being placed on duty without valid Georgia firearms licenses.
- Financial and administrative inconsistencies, including identified payroll discrepancies, invoicing errors, and failure to fulfill contract-required hours.

The COR responsible for managing the security guard contracts at the Carter Presidential Library documented his review of payroll to identify a shortage of service hours for June 2023. He also provided various other examples of contract performance issues throughout 2023. However, the last dated incident in the documentation NARA provided related to the termination of the contract is in January 2024, though the contractor's services continued through September 26, 2024. We could not corroborate the amounts invoiced for two of the three invoice line items in June 2024, and the documentation provided did not indicate prior awareness of these issues.

Because the COR responsible for managing the security guard contracts at Carter Presidential Library is no longer employed by the agency, we could not obtain further insight regarding the actions they regularly took to review and reconcile invoices, or whether they were previously aware of the June 2024 invoice discrepancies.

Reagan Presidential Library

Of the three selected Presidential Libraries, NARA provided the most complete records for the security guard contract at the Reagan Presidential Library. However, for 6 of the 12 selected months, NARA did not provide all invoices related to the additional services provided by the vendor.

Fixed-Price Services

For each of the 12 selected invoices, NARA provided the monthly report that the Reagan Presidential Library security guard contractor submitted for its required monthly deliverable. Eleven of the monthly reports contained detailed information related to the monthly performance of the contract, including daily records of time of arrival and departure for each security guard, by name, for fixed-price service hours provided during the month. Each monthly report also includes the total productive hours provided by the vendor. The monthly report for March 2023 contained only the daily time records associated with February 2023.

We compared the total hours from each of the 12 selected invoices to the 11 monthly reports that contained the daily time records associated with the selected month. We found that none of the hours on the invoices reconciled to the total hours on the monthly reports. Specifically,

- In 8 of 11 months, the daily time records in the monthly report were less than those included on the invoice. These discrepancies totaled 3,319.5 hours. Using the base-year hourly rate for additional services of $45.99, these discrepancies reflect potential questioned costs of $152,663.81.
- In 3 of 11 months, the daily time records in the monthly report were greater than those included on the invoice. These discrepancies totaled 289.25 hours. Using the base year hourly rate for additional services of $45.99, these discrepancies reflect potential underpayment of $13,302.61.

We could not compare the daily time reports to the contractually required fixed-price daily hours by position because the detailed records associated with the selected invoices do not include the position titles for each of the guards.

Additional Services

For each of the 12 selected months, the Reagan Presidential Library monthly reports also contained records of time of arrival and departure for each security guard, by name, for additional service hours provided for various events during the month. However, similar to the daily time records for the fixed-price services, the monthly report for March 2023 contained only the daily time records associated with February 2023.

At the Reagan Presidential Library, the additional services are invoiced separately from the fixed-price services. For the 11 selected months for which NARA provided daily time records, we found the following:

- For 5 of the 11 months, NARA provided invoices associated with additional services. For these invoices, we were able to reconcile all invoiced charges to the daily time records in the monthly reports.
- For 6 of the 11 selected months, NARA did not provide all invoices associated with additional services and, therefore, we could not reconcile all of the invoiced charges to the daily time records. However, for the invoices that NARA did provide, we did not identify any exceptions.

Truman Presidential Library

For each of the 12 selected invoices, NARA provided the monthly summary report and weekly "productive hours" report that the Truman Presidential Library security guard contractor submitted as part of its required monthly deliverables. The monthly summary report is a brief, one- to two-page document. These documents do not include a detailed list of guard employees and their position titles, or a list of the additional services provided in a given month.

The Truman Presidential Library security guard contract includes two CLINs associated with fixed-price services: one for Security Guard Services, or non-supervisory services; and one for Supervisor Services. We analyzed 46 productive hours reports associated with the 12 selected invoices. **Figure 2.** shows a blank version of this report.

Figure 2. Truman Presidential Library Productive Hours Report

Hours of Duty Worked		Report For Productive Hours Worked										
Security Service Contract Harry Truman -- IDS International, 2500 Wilson Blvd, Suite 200, Arlington, VA										Page 1	of	1
Month	November	Scheduled Tour								WEEKLY	REMARKS	
Employee's Name	**Position**	of Duty	M	T	W	T	F	S	S	TOTAL	(NOTE: for GSA Use)	
	Site Supervisor											
	Shift Supervisor											
Total Productive Hours Worked												
Total Productive Hours Required By Contract												
Variance (+ or -)												
Total Supervisory Hours Worked												
Total Supervisory Hours Required by Contract												
Variance (+ or -)												
To be completed by Contractor			To be completed by NARA Official									
Man hours have been provided in accordance with the minimum hourly requirements of contract number. I hereby certify the above to be correct.		Contract No. NAMA-21-F-00041	I hereby certify the above has been compared with the form 139 Record of time Arrival & Departure from Bldg (during Security hours) or other approved sign in/out form, & that discrepancies are noted above & will be referred to Contracting Officer									
Submitted by	Title	Date	Verified by							Date	Title	
ON SITE SUPV.												

Source: Sikich modification of Truman Presidential Library document to remove guard names and hours.

Each of the productive hours reports we evaluated included a full list of all guards employed by the contract. However, almost all of the reports only included position information for one Site Supervisor and one Shift Supervisor.[11] The position information for each of the other guards was left blank. Based on the identified position information, none of the 46 weekly reports included accurate totals for productive hours worked or supervisory hours worked. Specifically, we found:

- The contractor did not provide the minimum number of supervisory hours required for 45 of the 46 weekly reports.
- The contractor provided productive hours in excess of the contract requirements on 45 of the 46 weekly reports.
- For 27 of the 46 weekly reports, the total number of hours the contractor provided matched the total number of required hours. However, because the productive hours report did not identify the skill category of most of the guards, it is not possible to identify the hours they worked that could be reliably attributed to supervisory hours instead of productive hours.

[11] The February 2022 productive hours reports included a third Shift Supervisor.

- For the 19 weekly reports where there was an overall discrepancy with the required contract hours:
  - 3 weekly reports showed the contractor did not meet the minimum weekly required hours, reflecting a total deficit of 30.5 hours. Based on the hourly rate identified by the contract for additional services in FY 2022, this reflects a deficit from the agreed upon fixed-price services of $999.[12]
  - 16 weekly reports showed that the contractor provided a total 114 hours in excess of the contract requirement, reflecting $3,735 beyond the fixed-price services.

In addition, our comparison of the invoices to the relevant contract rates identified an instance in which the vendor overcharged for fixed-price guard services, resulting in questioned costs of $3,458.

According to the cognizant COR, the productive hours report appears to inaccurately record the different types of hours because it does not identify the nine other guards who can serve as a shift supervisor as needed. While we obtained the list of these individuals, because the productive hours report did not identify the skill category of most of the guards, it is not possible to identify the hours they worked that could be attributed to supervisory hours instead of productive hours. Without detailed monthly status reports containing daily hours logged by each individual within a specified skill category and CLIN for the reporting period, it is not possible to properly reconcile the invoices with the services actually provided.

According to the COR, the vendor maintains a more detailed work schedule, but it is not submitted as part of the monthly report. Further, the COR does not review the detailed work schedule or productive hours report when approving the fixed-price invoices, and instead checks that the invoice amount matches the monthly fixed-price total for the given contract option year.

None of the cognizant CORs for the three selected Presidential Libraries reconciled monthly invoices with detailed daily time reports that included the service hours provided by skill category and CLIN. Establishing a process that requires the COR to reconcile the invoices with the required monthly documentation would not only help ensure that the vendor is meeting all contract service and deliverable requirements, but it would also help to prevent potential overcharges, such as the potential $158,880.29 in questioned costs that we identified.

Therefore, we recommend NARA's Executive for Business Support Services in coordination with the Acquisitions Division (BZ) Director and the Executive for Presidential Libraries:

> ***Recommendation 3:*** Require that CORs document their reconciliation of invoices with detailed timesheets before security guard contract invoices are paid.
>
> ***Recommendation 4:*** Recover or otherwise resolve the $158,880.29 in questioned costs from security guard vendors.

In addition, we recommend NARA's Executive for Business Support Services, in coordination with the BZ Director:

[12] The additional services rate for FY 2022 was $32.76.

Recommendation 5: Provide training on the new documentation requirements to any COR responsible for security guard contracts.

Finding 4: NARA Approved Unallowable Costs at the Truman Presidential Library

In addition to the fixed-price services at the Truman Presidential Library described in Finding 3, 6 of the 12 sampled invoices included charges associated with additional services. For additional security guard services for special events, the vendor submits a Form NA 5007 (7-88), *Requisition for Equipment, Supplies, or Services,* which is noted as received by the COR following the completion of the event. The COR then tracks each expense in a spreadsheet that covers the entire contract year.

The security guard contract for the Truman Presidential Library requires the vendor to supply all training, equipment, materials, and supplies necessary to staff and operate and provide routine and emergency protective and security support services. The contract states that the vendor is responsible for furnishing all items of uniform and equipment necessary to perform required work, including ammunition, firearms, and associated holsters, belts, and firearm belt accessories. In the contract years from 2023 through 2025, the Truman Presidential Library used funds from the additional services CLIN to purchase unallowable materials for the security guard contract, as shown in **Table 1**.

Table 1. Materials Purchased through the Truman Presidential Library Security Guard Contract

Date	Materials Purchased	Amount
2/28/25	Firearms Training Ammunition	$3,701.85
3/21/24	Additional Training Supplies	$2,403.00
3/15/23	Replacement Holsters & Training Ammo	$2,988.80
Total		**$9,093.65**

According to the cognizant COR, these purchases were made at the end of the contract year after all additional services have been met and paid for. The COR explained that at the end of the contract year, when funds remain in the additional services CLIN, the vendor can submit a Form NA 5007 (7-88), which is the same form submitted for special event security guard services. This practice was in place because the contract clause associated with the additional services does not explicitly prohibit the use of the additional services CLIN for materials or supplies. However, Form NA 5007 (7-88) clearly states, "The contract specifications and requirements govern the above additional services ordered."

As a result of these costs that do not comply with the contract terms, NARA incurred $9,093.65 in questioned costs. These costs represent expenditures that were unallowable under the current contract terms.

Therefore, we recommend NARA's Executive for Business Support Services, in coordination with the BZ Director and the Executive for Presidential Libraries:

Recommendation 6: Recover or otherwise resolve the $9,093.65 in questioned costs from the security guard vendor at the Truman Presidential Library related to unallowable supply and material charges.

Recommendation 7: Provide specific guidance to CORs responsible for security guard contracts or, as appropriate, issue a contract modification which further clarifies the

allowable uses for the "Additional Services" CLINs, and processes required to use available funds for other purposes.

OTHER MATTERS

During our audit of NARA's Security Management program, we made a related observation that was outside the scope of our audit. Specifically, we found that the Facility Security Level (FSL) that the Federal Protective Service (FPS) assigned to the Atlanta Federal Records Center (FRC) in February 2025 was not justified.

On October 1, 2024, the GSA assumed the leasing authority for the Atlanta FRC facility.[13] When GSA assumes leasing authority, FPS becomes responsible for the facility's security and conducts a new Facility Security Assessment (FSA). According to NARA officials, after GSA assumed the leasing authority for the Atlanta FRC, they were informed that GSA requirements for certain security measures for FSL II facilities differed from those implemented by NARA BX. Consequently, GSA informed NARA BX that if they wanted to continue with the same security measures, NARA would be required to fund them.

To continue with the security measures preferred by NARA BX without incurring the costs, NARA management requested that FPS increase the FSL designation from Level II to Level III. On February 3, 2025, FPS issued a new FSA for the Atlanta FRC, which included a new FSL score of Level III.[14]

To accomplish the change in FSL, FPS revised NARA's previous FSL determination by increasing the Facility Size score from "2" to "4" and the Threat to Tenant Agencies score from "2" to "3." The change to the Facility Size score corrected the inaccuracy we reported on in Finding 1.[15] However, without also increasing the Threat to Tenant Agencies score, the Atlanta FRC would have retained the Level II designation. In their request to FPS related to increasing the FSL to Level III, NARA stated that the reason for the request was to ensure they could continue with a security practice that is not considered standard FPS for Level II facilities. However, NARA did not provide any information that indicated the areas associated with the Threat to Tenant Agencies score had changed. Further the information provided within the FPS FSA does not indicate any changes in any of the following areas:

- Contact with the public,
- Mission,
- Past and current credible threats, or
- Crime statistics.

Unsupported changes to FSL factor scores because of financial concerns compromise the integrity of the risk management process. For example, in its FSA, FPS identified a security deficiency at the facility based on the standard measures it implements at Level III facilities, and estimated the annual cost of implementing the requirement to be $244,000 – $500,000. However, despite specifically requesting the FSL be changed to Level III, NARA management

[13] The transition from NARA's BX to FPS as the responsible security organization was occurring during audit fieldwork. We had previously determined that the other GSA-owned or -leased facilities within our sample that had FSAs conducted by FPS were outside the scope of the audit. However, we were not made aware of the Atlanta FRC change in security organizations until our site visit in February 2025.
[14] While FPS finalized the FSA in February 2025, all parties agreed to the initial revised FSL in November 2024.
[15] The Atlanta FRC is 352,064 square feet. The ISC standards requires facilities with a size of greater than 250,000 square feet be assigned a score of "4", whereas the 2023 NARA FSA assigned a score of "2".

declined to implement this Level III security requirement from the Atlanta FRC's 2025 FSA. Without an objective FSA, NARA management lacks assurance that the recommended and implemented security measures are commensurate with the needs of the facility.

MANAGEMENT COMMENTS AND OUR EVALUATION

We provided a draft copy of this report to NARA management for review and comment. Management provided written comments, which are included in Appendix B, and technical comments, which we incorporated as appropriate. In its written comments, management concurred with all seven of Sikich's recommendations. In addition, management identified further related actions it intends to take beyond each of the original recommendations.

APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this performance audit was to evaluate the efficiency and effectiveness of NARA's Security Management program and determine whether guard contract vendor payments made by NARA at selected Presidential Libraries were reasonable and properly supported by services provided, in accordance with contractual provisions.

Scope

The scope of the audit included NARA's security management program across selected facilities in FYs 2022 through 2024. In addition, the scope includes security guard contracts and agreements at selected Presidential Libraries. This report is a public version of a sensitive report issued in January 2026. This report omits specific details regarding security measures, threats, and vulnerabilities, which could pose unintended security risks. Although the information provided in this report is more limited, the report addresses the same objectives as the report containing sensitive information and uses the same methodology.

Methodology

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards* (2018 Revision, Technical Update April 2021). 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 objectives. We conducted the audit fieldwork in Alexandria, Virginia; Atlanta, Georgia; Kansas City, Missouri; Riverside, California; Simi Valley, California; Yorba Linda, California; St. Louis, Missouri; College Park, Maryland; Washington, DC; and remotely from September 2024 through November 2025.

To accomplish our audit objectives, we completed the following procedures:

- Obtained and reviewed applicable federal regulations, standards, and NARA policies and procedures related to security management requirements, including but not limited to:
    - Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Interagency Security Committee Standard, *The Risk Management Process* (2024 Edition).
    - Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Interagency Security Committee, Appendix A: The Design-Basis Threat Report- The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (2023 Edition).
    - Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Interagency Security Committee, *Appendix B: Countermeasures- The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (2023 Edition).
    - GAO, Standards for Internal Control in the Federal Government (Green Book), (September 2014).

- Executive Order 12977 Executive Order on Interagency Security Committee (November 27. 2023).
- NARA's BX Facility Security Risk Management Program IOP (December 6, 2024)
- Executive Order 14111 Interagency Security Committee, (November 27, 2023)
- NARA Archives II A2-BX Occupant Emergency Plan Emergency Response IOPs, (February 28, 2024)
- NARA Directive 204, Access Privilege Procedures at AI and AII (May 26, 2011).
- NARA Directive 211, Exit Inspections of Property at NARA (August 2, 2022).
- Federal Acquisition Regulation 48 CFR § 4.803(a)(26) (2025)

- Conducted interviews with relevant NARA officials (e.g., Security Management Division, Research Services, Agency Services, and Presidential Libraries) throughout the engagement to obtain an understanding of NARA's physical security processes, including how roles are assigned and delegated, and oversight and monitoring is performed of security management at NARA facilities.
- Selected a nonrepresentative sample of 15 FRCs, Research Facilities, and Presidential Libraries based on location, facility type, FSL, and facility size, among other things. The selected facilities are shown in Table 2.

Table 2. Selected NARA Facilities

Area	Facility Name	Facility Type	Square Feet
Washington, DC:	National Archives I Washington DC	Research Facility	790,000
	Washington National Records Center	FRC	877,000
	National Archives II College Park, MD	Research Facility	1,374,384
California:	Riverside Archives and Federal Records Center	FRC and Research Facility	183,400
	Nixon Presidential Library	Presidential Library	118,173
	Reagan Presidential Library	Presidential Library	178,000
Missouri/ Kansas:	Kansas City Archives	Research Facility	35,911
	Truman Presidential Library	Presidential Library	105,000
	Kansas City Federal Records Center	FRC	385,169
	Lee's Summit Federal Records Center	FRC	806,794
	Lenexa Federal Records Center (Kansas)	FRC	982,644
	National Personnel Records Center and National Archives at St. Louis	FRC and Research Facility	474,688
Georgia:	Carter Presidential Library	Presidential Library	70,000
	Atlanta Federal Records Center	FRC	352,064
	Atlanta Archives	Research Facility	46,000

- Conducted site visits to the selected NARA facilities which included the following activities:
    - Interviewed the facility director, security officer, and other staff who support or manage facility security controls.
    - Identified and observed the entry and exit of employees, visitors, and contractors through the main entrance and all entry and exit points to the facility.
    - Conducted facility walkthroughs to observe key physical security countermeasures.
- Obtained and analyzed incident reports from the selected NARA facilities, to understand the types of incidents that occurred at the selected facilities, the process security officials used to document and maintain incident reports, and how, if at all, the facilities reported the incidents to BX.
- For the Carter, Reagan, and Truman Presidential Libraries, we examined guard contracts, monthly status reports, timesheets, and invoices to determine whether vendor payments made by NARA were reasonable and properly supported by services provided, in accordance with contractual provisions. We selected a random sample of 12 invoices for each location as the basis of our analysis.

We assessed internal controls that we deemed to be significant to the audit objective. Specifically, we assessed 12 of the 17 principles associated with the 5 components of internal control defined in GAO's *Standards for Internal Controls in the Federal Government* (September 2014) (the Green Book). Table 3 summarizes the principles we assessed:

Table 3: GAO Green Book Assessment Principles

Control Environment
Principle 3: Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
Risk Assessment
Principle 6: Management should define objectives clearly to enable the identification of risks and define risk tolerances.
Principle 7: Management should identify, analyze, and respond to risks related to achieving the defined objectives.
Principle 8: Management should consider the potential for fraud when identifying, analyzing, and responding to risks.
Principle 9: Management should identify, analyze, and respond to significant changes that could impact the internal control system.
Control Activities
Principle 10: Management should design control activities to achieve objectives and respond to risks.
Principle 11: Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
Principle 12: Management should implement control activities through policies.
Information & Communication
Principle 13: Management should use quality information to achieve the entity's objectives.
Principle 14: Management should internally communicate the necessary quality information to achieve the entity's objectives.

Monitoring
Principle 16: Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
Principle 17: Management should remediate identified internal control deficiencies on a timely basis.

We assessed the design, implementation, and/or operating effectiveness of these internal controls and identified deficiencies that we believe could affect NARA's ability to effectively manage NARA's security management activities. We discuss the internal control deficiencies we identified in the Audit Results section of this report. However, because our review was limited to aspects of these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this performance audit.

APPENDIX B: MANAGEMENT RESPONSE

January 22, 2026

Dear Inspector General Brown:

Thank you for the opportunity for NARA's executive leadership to review and comment upon the recent performance audit report ("Report") of NARA's security management program (SMP) for FY 2022 to FY 2024. We have carefully reviewed the Report's findings as to NARA's efficiency and effectiveness, or rather very disappointing lack thereof, in administering its SMP for FY 2022-2024. The findings expose significant and unacceptable weaknesses in NARA's security management program. The findings also establish a disturbing lack of oversight of the contracts and funds used for contracted security guards at various NARA facilities. We therefore thoroughly reviewed the Report's eight sets of recommendations for how NARA can strengthen its security management program and its oversight of security guard contracts and funds.

In short, NARA's executive leadership fully supports and intends to implement (if we have not already done so) each and every one of the Report's numerous recommendations for improving NARA's security management program and oversight of its security guard services. However, we strongly believe NARA, including NARA's Office of Inspector General (OIG), can and should and must do more to fix NARA's significant security lapses and wholly inadequate oversight of security guard contracts and funds. Americans deserve much better stewardship of the resources provided to NARA, and NARA should instead be using any funds lost to fraud or waste for its significant, mission-critical needs such as digitizing Presidential and federal records and maintaining its archival and Presidential Library facilities.

We therefore strongly recommend that the following additional steps be taken by NARA, the OIG, or both, to find and recover additional previously misspent or misused security guard contract funds, to strengthen NARA's current security management program, and to improve NARA's future oversight of its security guard contracted services:

Additional Recommendation No. 1 -- Once the Report's recommendations are implemented for improving the process of Facility Security Level (FSL) determinations and Facility Security Assessments (FSA) determinations, and for requiring critical documentation to accompany FSL and FSA determinations, NARA's Security Management Division Director (SMDD) should ensure every FSL and FSA determinations for each of NARA's 40 facilities, including but not limited to each of its Presidential Libraries, is reviewed, amended as appropriate, and adequately documented.

Additional Recommendation No. 2 -- Once the Report's recommendations are implemented for centrally obtaining, tracking, and analyzing each and every significant security risk and each and every significant security incident report across the agency, NARA's SMDD and NARA's Executive for Business Support Services (EBSS) should (1) regularly review, assess, and analyze the up-to-date central database containing all of the significant security risks and significant security incident reports from every facility across the agency; (2) understand and summarize the nature of the evolving security threats and risks facing NARA across the agency and make any necessary adjustments and helpful upgrades to NARA's security programs; and (3) report regularly to NARA's executive leadership about any significant security risks faced by NARA, the evolving nature of any significant security threats to NARA, and any implemented or recommended adjustments or upgrades to NARA's security programs. In addition, the SMDD and EBSS should immediately undertake a thorough and current security risk and threat assessment in preparation for NARA's and any NARA-sponsored America 250 activities, the results of which should be reported to NARA's executive leadership no later than March 30, 2025.

Additional Recommendation No. 3 -- Once the Report's recommendations are implemented to expressly require COR's to regularly reconcile and document the reconciliation of security guard contract invoices with detailed timesheets before any security guard invoices are paid by NARA, NARA's Chief Acquisition Officer should ensure that complying with the new reconciliation requirements be made a critical part of each COR's annual performance plan for all contracts, not just security guard contracts.

Additional Recommendation No. 4 -- While NARA and the OIG work cooperatively to recover or otherwise successfully resolve the audit-discovered $158,880.29 in questioned costs from the security guard vendors at the three selected Presidential Libraries, (1) the OIG should undertake and complete comprehensive audits and/or investigations of every security guard vendor and contractor at every Presidential Library and at every other applicable NARA facility for at least the past three or four years to find any additional questioned costs; (2) the OIG and NARA should work cooperatively to recover or otherwise successfully resolve any additional audit-discovered or investigation-discovered questioned costs; and (3) the OIG and NARA should work cooperatively to appropriately punish and recover any damages for any fraudulent behavior, false claims, or otherwise improper conduct by any security guard contractor or NARA employee involved with the security guard contractors or contracts.

Additional Recommendation No. 5 -- While NARA provides training on the new documentation requirements for all COR's responsible for security guard contracts, NARA's Chief Acquisition Officer should ensure that complying with the new documentation

requirements be made a critical part of each COR's annual performance plan for all contracts, not just security guard contracts.

Additional Recommendation No. 6 -- While NARA obtains the required contract documentation associated with the security guard contract for the Reagan Presidential Library, and provides such documentation to the OIG, NARA's Chief Acquisition Officer should ensure that any and all required contract documentation for every security guard contract for every Presidential Library and any other applicable NARA facility is appropriately maintained in the applicable contract file.

Additional Recommendation No. 7 -- While NARA and the OIG work cooperatively to recover or otherwise successfully resolve the audit-discovered $9093.65 paid for unallowable supply and material charges to the security guard contractor at the Truman Presidential Library, (1) the OIG should undertake and complete an investigation of every "Additional Services" payment to any security guard contractor at every Presidential Library and at every other applicable NARA facility for at least the past three or four years to find any additional payments for unallowable expenses; (2) the OIG and NARA should work cooperatively to recover or otherwise successfully resolve any additional similar investigation-discovered payments for unallowable costs; and (3) the OIG and NARA should work cooperatively to appropriately punish and recover any damages for any fraudulent behavior, false claims, or otherwise improper conduct by any security guard contractor or NARA employee involved with the security guard contracts.

Additional Recommendation No. 8 -- While NARA provides specific and clarified guidance to all COR's about allowable and unallowable uses for "Additional Services" in security guard contracts and issues any necessary corresponding contract modifications for any security guard contracts, NARA should (1) determine whether any NARA employee intentionally allowed payments for unallowable expenses relating to any security guard contract for the past three or four years; (2) should appropriately punish any such NARA employee; and (3) should refer, where appropriate, the NARA employee (whether current or former) and the intentional conduct to the OIG for any additional appropriate investigation and punishment.

Recommendation for the Atlanta Federal Records Center (FRC) -- NARA's Executive Leadership believes the OIG and/or NARA should (1) determine whether any NARA employee intentionally engaged in any misconduct by seeking a higher security rating for the Atlanta FRC, by refusing to pay for the necessary security resources required of an upgraded-security-level Atlanta FRC, or by both; and (2) appropriately punish any such NARA employee for any intentional misconduct.

Background Section (page 3): We propose editing the first few sentences of the first paragraph of the Background section to say as follows: "NARA is a distinct federal agency within the Executive Branch of the United States government responsible for preserving, protecting, and providing access to the records of our federal government. NARA's mission is to preserve, protect, and share the historical records of the federal government to promote public inquiry and federal government accountability. As of 2005, ..."

Signed by: Valorie Findlater

APPENDIX C: ACRONYMS

Acronym	Definition
BX	Security Management Division
CLIN	Contract Line Item Number
DBT	Design Basis Threat
DHS	Department of Homeland Security
FPS	Federal Protective Service
FRC	Federal Record Centers
FSA	Facility Security Assessment
FSL	Facility Security Level
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
ISC	Interagency Security Committee's
IOP	Internal Operating Procedure
NARA	National Archives and Records Administration
OIG	Office of Inspector General
PIV	Personal Identity Verification
RMP	Risk Management Process
UE	Undesirable Events

APPENDIX D: OIG HOTLINE CONTACT INFORMATION

The OIG Hotline provides a confidential channel for reporting fraud, waste, abuse, and mismanagement to the OIG. In addition to receiving telephone calls at a toll-free Hotline number, we also accept emails through an online referral form.
Visit https://naraoig.oversight.gov/ for more information, or contact us:

Contact the OIG Hotline
Online Complaint Form | Office of Inspector General OIG

Contact the OIG by telephone and FAX
Hotline Telephone: 301-837-3500 (Local) or 1-800-786-2551 (toll-free)
FAX: 301-837-3197

Contractor Self-Reporting Hotline
As required by the Federal Acquisition Regulation, a web-based form allows NARA contractors to notify the OIG, in writing, whenever the contractor has credible evidence a principal, employee, agent, or subcontractor of the contractor has committed a violation of the civil False Claims Act or a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations in connection with the award, performance, or closeout of a contract or any related subcontract. The form can be accessed through the OIG's home page or found directly at OIG Contractor Reporting Form | Office of Inspector General OIG