Smithsonian Institution
Office of the Inspector General

In Brief

Physical Security and Inventory Control Measures to Safeguard the National Collections at the National Air and Space Museum

Report Number A-09-04, March 17, 2010

Why We Did This Audit

We conducted this audit to determine whether (1) physical security is adequate to safeguard the collections and (2) inventory controls are in place and working adequately to ensure that the collections are properly accounted for at the National Air and Space Museum (NASM). The audit is the latest in our series covering collections at the Smithsonian.

What We Recommended

We made ten recommendations to bring collection areas up to Office of Protection Services (OPS) standards and strengthen the physical security of NASM's collections. We made five recommendations to strengthen inventory controls. Management mostly concurred with our findings and recommendations and has planned corrective actions that resolve most of our recommendations.

What We Found

We believe NASM's physical security is generally adequate to safeguard the collections, but that the Office of Protection Services (OPS) needs to strengthen protection of high-security collection storage areas. We found that OPS had not installed required security devices in all of these areas, and some security controls were frequently malfunctioning or inoperable. These breakdowns increase the risk of theft and diminish control over collections. If thefts were to occur, it would be difficult to identify when and how they took place.

We found that inventory controls were not fully in place. NASM staff has not conducted cyclical inventory reviews as required by NASM policies and did not maintain complete inventory records. Yet, we confirmed that NASM could account for the collection objects in the statistical sample we tested.

The results of this audit were similar to the results of an audit of National Museum of Natural History (NMNH) collections, where we also found security and inventory problems. The results of both audits show the persistence of the collections issues noted in the 2005 report ***Concern at the Core: Managing Smithsonian Collections***. We are concerned that five years have passed since that report and almost four years since we issued our report on NMNH. We hope that the Institution's Strategic Plan objective to strengthen collections stewardship signals increased attention to safeguarding the collections.

In its response to our audit, Smithsonian management maintained that collections are not at risk and objected to fixing security problems piecemeal. Management would prefer to address security deficiencies in the context of Institution-wide risks and conduct upgrades and repairs only in larger capital projects. OPS would also prefer to be guided by an Institution-wide collections storage plan, but such a plan does not yet exist. We believe the Smithsonian must prudently balance its collections security funding decisions against its long-term strategic goals.

For additional information or a copy of the full report, contact the Office of the Inspector General at (202) 633-7050 or visit http://www.si.edu/oig.

Smithsonian Institution

Office of the Inspector General

Date March 17, 2010

To John R. Dailey, Director, National Air and Space Museum
Bruce Kendall, Director, Office of Facilities Engineering and Operations
James J. McLaughlin, Director, Office of Protection Services
Andrew J. Zino, Comptroller

cc Doug Hall, Associate Director, Technical Security Division, Office of Protection Services
Peter Jakab, Associate Director, Collections and Curatorial Affairs Department, National Air and Space Museum
Elizabeth Garcia, Chief, Collections Division, National Air and Space Museum
William Tompkins, National Collections Coordinator

From A. Sprightley Ryan, Inspector General

Subject Audit of Physical Security and Inventory Control Measures to Safeguard the National Collections at the National Air and Space Museum, Number A-09-04

This report, a continuation of our series covering collections at the Smithsonian, presents the results of our audit of security and inventory control measures over the collections at the National Air and Space Museum (NASM). The Office of the Inspector General (OIG) initiated this audit to examine these two aspects of collections management, which are essential for safeguarding the collections for public and scholarly use and reducing the risk of loss or theft. An earlier audit covered the National Museum of Natural History (A-05-06, September 29, 2006); the next audit in the series will cover the National Museum of American History collections.

Collections are at the core of the Smithsonian. The Smithsonian Strategic Plan for fiscal years 2010-2015 states: "The collections are fundamental to our work and to that of countless scholars and many federal agencies; it is our responsibility to preserve them for future generations. To ensure they remain available, we will improve collections storage and management..."

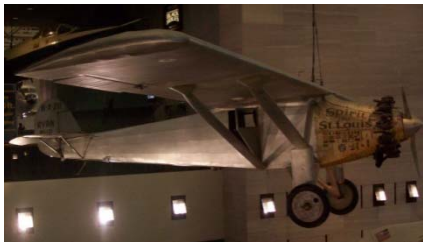
Our objectives in this audit were to determine whether (1) physical security is adequate to safeguard the collections, and (2) inventory controls are in place and working adequately to ensure that the collections are properly accounted for in compliance with Smithsonian and Museum collections management policies and procedures. We assessed the use and effectiveness of security devices throughout NASM; evaluated access to storage facilities; examined inventory controls; and identified missing or misplaced objects by testing inventories. We describe in detail our audit scope and methodology in Appendix A.

RESULTS IN BRIEF

We believe that NASM's physical security is generally adequate to safeguard the collections; however, improvements need to be made in some areas. We also found that inventory controls were not fully in place; yet, we found no collections objects unaccounted for in our limited statistical sample. We believe that OPS and NASM should

improve physical security and inventory controls to safeguard the collections. In particular, OPS needs to strengthen the effectiveness of controls over high-security collection storage areas. We found that the Smithsonian had not installed required security devices in all of NASM's high-security collections areas, and that some security controls were frequently malfunctioning or inoperable. These breakdowns increase the risk of theft and diminish control over collections. If thefts were to occur, it would be difficult, if not impossible, for the Smithsonian to identify when and how they took place.

In addition, we found that NASM staff have not conducted cyclical inventory reviews as required by the NASM Cyclical Inventory Plan and did not maintain complete inventory records. Despite the absence of cyclical inventory reviews, we were able to confirm through our own test work that NASM could account for the collection objects under its control. As part of our audit we conducted a spot-check inventory of a random sample of 366 accessioned objects. We located 360 of the objects; the other 6 were inaccessible.[1]



Charles Lindbergh's Spirit of St. Louis, NASM Mall Museum

(b) (2) [redacted] In the wake of the theft, NASM conducted extensive reviews of their collections to confirm that nothing further was missing. The benefits of their reviews carried forward to our own inventory test counts.

Information redacted pursuant to Freedom of Information Act Exemption 2 will be labeled "(b)(2)."

As noted in ***Concern at the Core: Managing Smithsonian Collections*** (April 2005), the Office of Policy and Analysis' (OP&A) comprehensive study of collections management at the Institution, Smithsonian collections are increasingly at risk because of declining resources to perform basic collections management. Our previous audit, ***Physical Security and Inventory Control Measures to Safeguard the National Collections at the National Museum of Natural History*** (NMNH), also found significant problems with the physical security and inventory controls at NMNH and reaffirmed the fundamental concerns over collections management presented in the ***Concern at the Core*** report. Accordingly, in that earlier audit, we recommended that NMNH follow the suggestions of the ***Concern at the Core*** and, more specifically, develop plans for a prioritized cyclical inventory; make inventory goals a part of collections managers' performance plans; and finalize the museum's inventory plan. The Director of NMNH generally agreed to all the recommendations from our report and followed through to implement substantially all of them.

We recognize the responsiveness on the part of NMNH officials to our recommendations and encountered a similar reaction from the officials at NASM while conducting our test work on the current audit. OPS officials moved promptly to remedy many of the security deficiencies as soon as we advised them of our concerns. OPS has drafted ***Collections Management Security Standards*** to guide collections stewardship and drive accountability down to the functional levels of the museums. We are encouraged by the comprehensiveness of such an undertaking. All the same, the similarity between the

[1] Six objects were inaccessible because four were installed on other objects on display, one was in a construction zone, and one was missing on account of a prior theft.

results of our prior audit and this one is troubling. Five years have passed since OP&A issued the ***Concern at the Core*** report and almost 4 years have passed since we issued the collections report at NMNH. Yet, neither report appears to have prompted a pan-Institutional focus on improved collections and security practices. The concerns that repeatedly surface in the course of our audit illustrate the continued urgency of improving collections and security management. We acknowledge that OPS and NASM must compete for scarce resources needed for other high-priority collections and security management improvements at the Smithsonian. However, as we continue to conduct audits of collections and security, we hope that Smithsonian management will advance its strategic objective of strengthening collections stewardship by continuing to press for funding to address the ongoing need for improved collections security across the Institution.

To ensure that physical security controls over access to the NASM collection storage areas are adequate, we recommended that the Smithsonian revise and implement its security policies and procedures, as well as ensure that budget requests reflect collection security priorities. To ensure that there are adequate inventory controls, we recommended that NASM conduct and document inventories according to their Cyclical Inventory Plan; include measurable goals for record completeness in curatorial performance plans; and establish an appropriate segregation of duties between access to collection records and objects.

BACKGROUND

NASM Collections

NASM, with the world's largest collection of historic aircraft and spacecraft, manages approximately 57,000 objects. Fewer than 5,000 of these objects are on exhibit at the NASM Mall museum and the Steven F. Udvar-Hazy Center (Hazy) in Chantilly, Virginia. The majority of the collection is in storage at the Paul E. Garber Facility (Garber) in Suitland, Maryland, and several small storage rooms at the NASM Mall Museum (see Appendix C for images of all the NASM facilities).

At NASM, care and accountability for the collections is the responsibility of the staff of the Collection and Curatorial Affairs Department. This Department comprises the following divisions: Aeronautics, Space History, Archives, the Center for Earth and Planetary Studies (CEPS), and Collections. The Collections Division includes the Preservation and Restoration, Conservation, and Collections Processing Units. The Collections Division is responsible for the physical care of the collections and other activities such as storage, loans, transportation, and maintaining collection records. The curatorial staff is responsible for the intellectual attributes of the collection, including deciding which objects to collect and display. NASM collections are assigned to one of four divisions: Aeronautics, Space History, Art, and CEPS. The following table shows how many accessioned objects each division is responsible for:

Division	# of Objects
Aeronautics	37,622
Space History	14,827
Art	4,245
CEPS	10
No Division Assigned	13
TOTAL	**56,717**

NASM Collection Storage Areas

Mall Museum - [redacted] These storage areas account for approximately 8,600 (about 15 percent) accessioned objects. Additionally, approximately 1,850 objects are on display (or installed on other objects on display) in the museum's 22 galleries.

Garber Facility - The Paul E. Garber Facility[2] is made up of 34 metal buildings, some of which date from the 1950s, 23 of which are used by NASM. NASM stores the majority of its collections (39,000 out of 57,000 objects) at Garber. [redacted]

Hazy Center - The Steven F. Udvar-Hazy Center currently does not have space dedicated to object storage. All its nearly 3,000 objects are on display in its two hangars: the Boeing Aviation Hangar and the James S. McDonnell Space Hangar. The second phase of the Hazy Center is currently under construction. It will include a collection storage facility and is expected to open in 2011. NASM will relocate the restoration, conservation, and collections processing units, as well as approximately 36,000 objects, from the Garber Facility to the expanded Hazy facility. There is additional storage of over 100 objects in a hangar located on Washington Dulles International Airport property; a C-130 aircraft is also being stored outside the hangar.

C-130 stored outside the "Shuttle Hangar" at Washington Dulles International Airport.

[2] The Garber Facility is one of three facilities at the Smithsonian's Suitland, Maryland site; the other facilities are the Museum Support Center (MSC) and the Cultural Resources Center (CRC).

NASM Security

The Office of Protection Services (OPS) is responsible for the security of staff, visitors, and collections Institution-wide. OPS is a branch of the Office of Facilities Engineering and Operations (OFEO). OPS provides protection and security services and operates programs for security management and criminal investigations at Smithsonian facilities on and near the National Mall in Washington, DC, New York City, and Panama. Each building or compound has a Security Manager who is in charge of overseeing security for that location. The Security Manager reports to the Area Security Manager, who is responsible for overseeing multiple facilities in a geographic area.

The Technical Security Division (TSD) of OPS provides technical assistance and advisory services to SI bureaus, offices, and facilities, as well as maintains and repairs all technical security equipment, such as door access-card readers, cameras, and motion detectors, throughout the Institution. TSD also provides security design and construction support. The System Administration Section of TSD coordinates the repair of system or device failures, preventative maintenance, maintenance contracts, system inspections, and system changes (due to construction or exhibits). Another component of TSD is the Locksmith Shop, which provides all lock and key services to facilities and OPS Security Units and Divisions throughout the Smithsonian. The Office of the Comptroller (OC) is responsible for exit clearance procedures.

Process for Security Improvement

The Smithsonian's Capital Planning Board, with input from Smithsonian's senior leaders, decides which security upgrades it will fund in the course of the annual capital planning process. The Board identifies and prioritizes capital projects, some of which may include major security upgrades to Smithsonian buildings. OPS' Technical Security Division specifies security requirements for these projects based on its security assessments. According to OPS, the Technical Security Division rarely requests security projects that are not part of a larger capital project unless there is a compelling need, because of the inefficiency of managing many smaller security projects.

The Office of Policy, Planning, and Maintenance, in conjunction with other OFEO components, is responsible for ensuring that construction contractors properly install devices that meet OPS security specifications.

RESULTS OF AUDIT

Security of the Collections Does Not Meet OPS Standards

The Smithsonian has not installed required security devices in all of NASM's high-security collections areas. The missing security devices diminished controls to prevent and detect theft of collections. If thefts do occur, it will be difficult, if not impossible, for the Smithsonian to identify when and how the thefts occurred or who was involved because there would be no electronic or video record of who accessed the collection area.

OPS ***Protective Design Standards for Technical Security*** (revised December 2004) includes specific minimum technical security requirements for all existing collection storage areas. The standards require the installation of cameras, intrusion-detection (motion) sensors,

card readers, door contacts, and other security devices based in part on the value of the collection to be protected. During our audit, OPS issued revised design standards[3] that apply only to newly constructed facilities and other facilities undergoing major renovations, and require that risk levels be assigned to collection storage areas to help identify appropriate security devices. We evaluated collection storage areas using both standards and found the same results using either set of standards.

In addition, the OPS Staff Security Handbook requires OPS to commission risk assessments of all major Institution facilities on a three- to five-year cycle. The purpose of these assessments is to identify areas of vulnerability so that OPS can update or refine security measures. These measures usually entail capital or maintenance projects or improved practices and procedures.

In addition to risk assessments, the OPS handbook requires that OPS conduct security management surveys of Institution facilities. The purpose of these surveys is to ensure Institution facilities comply with proper operational procedures, policies, and security standards. Additionally, OPS can use the surveys to identify new mitigation, operational, and physical security measures to reduce risk.

Lack of Security Devices in High-Security Collections Areas

We conducted a detailed review of all the high-security collections areas and determined that no single area had all the security devices that are required by OPS standards.[4]

The Smithsonian did not install security devices to the extent required by OPS standards because:

- OPS's practice for requesting security upgrade funding is primarily tied to capital projects. OPS management explained that they are aware that they are not in compliance with their security standards; however, they believe that the necessary upgrades will be addressed as new capital projects are completed. OPS has not requested any capital funding for NASM collections storage projects because OPS management did not believe that the risk to NASM collections was significant when compared to the overall security risks facing the Institution as a whole.

- Although required to perform the risk assessments and security management surveys by the OPS Handbook, OPS had not conducted these formal assessments for the NASM Mall location or the Udvar-Hazy Center in Virginia. They had performed a security management survey at Garber in 2006; however, this assessment did not include all storage locations. OPS management told us they had conducted informal security assessments but had not documented these efforts. OPS management told us they believe that their informal inspections of NASM Facilities provide them with adequate awareness of the risks.

- [redacted] (b) (2) [redacted]

[3] Smithsonian Institution Security Design Criteria, March 27, 2009.
[4] We briefed OPS and NASM at the time of our testing and subsequently provided them with a detailed list of which security devices were lacking in which areas (Management Advisory No. M-09-04, Sept. 18, 2009).

Security devices such as card readers and cameras provide an electronic record of who accessed an area, when it was accessed, and where the access took place. In the event of a theft, information recorded by these devices would be essential to an investigation. Failure to implement these standards exposes the museum to an increased risk of theft, loss, or damage to objects, especially in areas where valuable and sensitive collection objects are stored.

RECOMMENDATIONS

To bring all collection storage areas up to OPS standards and to strengthen physical controls over access to the collection storage areas, we recommend that the Director, OPS:

1. Conduct security assessments of the NASM, Hazy, and Garber facilities and develop a plan, in the context of overall Smithsonian funding priorities, to acquire missing security devices.

2. Ensure that OPS budget requests reflect the priorities identified in security assessments, including installations of required security devices in high-security areas across the Institution.

3. Finalize and issue the OPS ***Collections Management Security Standards***.

Improperly Functioning Security Controls

Similar to what we reported from our audit of NMNH, security controls at NASM facilities were often malfunctioning or inoperable. [redacted] (b) (2) [redacted]

[redacted] (b) (2) [redacted] Multiple priorities and limited funding have prevented OPS from replacing or upgrading security and mechanical devices. We also found that OPS inspections of high-security areas have not always identified malfunctioning security devices and have not always included all high-security areas.

In addition to malfunctioning security devices, we discovered that OPS and NASM personnel maintained inadequate control over keys to NASM facilities, resulting in reduced control over access to secure areas. We had noted similar problems at NMNH, where [redacted] (b) (2) [redacted]

Last, we found that security personnel did not fully utilize the security management systems, which are intended to integrate security cameras, video recorders, fire alarms,

and intercoms into a comprehensive surveillance system. As with missing security devices, malfunctioning security controls increase the risk of theft and diminish control over collection areas. We had found similar problems at NMNH: the security systems functioned properly but security personnel did not use them for their intended purpose.

Along with OPS' ***Protective Design Standards for Technical Security,*** the ***TSD High Security Area Inspection and Maintenance Program*** requires that TSD conduct tests of high-security areas quarterly to ensure that all devices are installed and working properly.

The OPS policy ***Lock and Key Management, OPS-48*** (revised August 2007) requires that when an employee leaves the Institution or a department, Security Managers return all Smithsonian keys assigned to that employee to the Locksmith. In addition, the policy requires Security Managers to request a Key Holder List from the Locksmith on a semiannual basis and confirm the accuracy of the list. As we previously reported in our audit of NMNH collections and security, the American Association of Museums' ***Suggested Guidelines for Museum Security***[5] call for museums to maintain a written security policy and to practice sound key control and retrieval. The ***Guidelines*** state that, at a minimum, all keys issued should be signed for on a register; there should be a key retrieval system to make sure all keys are returned when an employee leaves; all keys should be stored in a secure space and not be removable without authorization; and one person should be responsible for key control, issuance, and retrieval. Current OC employee exit procedures do not require turning in keys prior to separation from the Smithsonian.

Improperly Functioning Security Devices

We observed that many of the security devices at the high-security collections areas for both the NASM Mall and Garber locations were inoperable. [redacted] (b) (2) [redacted] We notified TSD staff, who in turn corrected some, but not all, of the malfunctioning devices.[6]

Weak Controls Over Keys

Keys from one NASM employee's office, including keys to offices, collection storage areas, and filing cabinets

Neither OPS nor unit personnel adequately controlled keys, diminishing the effectiveness of locked doors as a security device. At the Mall Museum, the Locksmith had issued more than 1,380 keys to 258 doors as of May 2009. The Key Holder List was not always updated when keys were transferred between employees. We examined the NASM Mall Key Holder List, and identified numerous individuals who no longer work for NASM, have transferred to a different SI unit, or are deceased. Further, the key list only contains the names of employees who received keys directly from the Locksmith. It does not include individuals who received keys from their

[5] These guidelines were adopted by the Museum Association Security Committee of the American Association of Museums and the Standing Committee on Museum, Library, and Cultural Property Protection of the American Society for Industrial Security, Revised 2002.
[6] We provided OPS with a list of the specific devices on Sept. 24, 2009.

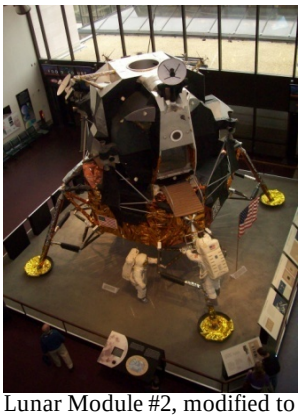
supervisors, other staff, or the museum security office. In addition, the Locksmith's report contained incorrect room numbers because NASM re-numbered the Mall museum's rooms approximately 10 years ago and did not provide updated information to the Locksmith. Consequently, we could not determine which rooms could be opened by the outstanding keys.

At the Garber facility, we determined that the Locksmith issued 41 out of 63 keys to a single employee for distribution to other staff. Approximately half of these keys were master keys that allowed access to collection storage areas. However, the employee did not know who at present was in possession of the keys.

At Hazy, although there are currently no collection storage areas, we found that the Security Managers were not confirming that employees listed on the Key Holder List could account for any of the 150 keys issued to them.

OPS Security Management System Needs Improvement

We found that OPS security management systems for the NASM facilities need improvement. Physical access to NASM facilities is controlled by security systems that are a combination of security devices and application software. The application software gathers data from devices such as cameras, card readers, motion sensors, and alarms. The systems alert security staff to actionable events such as alarms and document the acknowledgement and actions taken to resolve the events. The software also controls access based on a user authorization list programmed in its card readers. OPS uses one application software to manage its security devices at the Mall Museum, and another to manage devices at Garber and Hazy. We noted several problems with both systems that limit their usefulness in preventing and detecting unauthorized access. For example, some door contacts were improperly programmed, and some doors were improperly identified within the system.[7] We also found the following problems:


Lunar Module #2, modified to resemble Apollo 11 ***Eagle*** module, NASM Mall Museum

- **Lack of reports from the security system at the Mall Museum.** During our audit, TSD was unable to produce useful reports from the system at the Mall Museum such as Manual Action, Event, Access, and Rejection Reports.[8] Without these reports, security officials at the Mall Museum are unable to review normal access activity, unauthorized access, programming errors, or malfunctioning devices. According to TSD managers, they are now producing these reports and distributing them to security managers.

[7] We briefed OPS and NASM at the time of our testing and subsequently provided them with a list of the errors we found in the system (Management Advisory M-09-04, Sept. 18, 2009).
[8] Manual Action Reports show manual Control Room Officer actions such as deactivating a security device for a period of time. Event Reports show all alarm activity. Access Reports show all entries recorded by card readers including date/time, employee name, and location. Rejection Reports identify employees who were denied access to locations with card readers and include the same information as Access Reports as well as the reason for rejection.

- **Inadequate reporting from the system at Garber.** Manual Action and Event Reports produced by the system at the Garber Facility consolidate security activity from five separate locations into one report without organizing the results by location. Consequently, these exception reports are difficult to interpret, and security officials do not use them to oversee access to restricted facilities.

- **Software problems with the system at Garber.** In Spring 2009, software problems resulted in the system denying authorized staff access to buildings during their regular work hours. As a temporary solution, security granted staff 24-hour access to the buildings.

* * * *

These problems with the security systems were caused by the following:

- OPS high-security area inspections were not as rigorous as they should have been and thus failed to identify all malfunctioning and mis-programmed alarms. For example, we found that security officers routinely received and responded to an alarm that directed them to an incorrect location. A more comprehensive alarm inspection would have identified that the security system had not been programmed correctly. We note that the individuals who conducted the testing are the same individuals who are responsible for maintaining the security devices. We believe there should be a separation of duties, as a more objective review may help to identify problems with these devices. Moreover, OPS only tested the security devices at the three NASM facilities semi-annually, rather than quarterly as required by the ***TSD High Security Area Inspection and Maintenance Program*** in effect at the time of the audit.

- We also found a lack of management oversight or consistent policies over the assignment of keys to NASM staff. OPS policies require Security Managers to request a Key Holder List Report from the Locksmith on a semi-annual basis to confirm the accuracy of the list. However, none of the Security Managers were aware of this policy prior to our audit and thus had not requested or reviewed the Key Holder List nor reconciled discrepancies. In addition, they did not notify the Locksmith Shop of room number changes.

  OPS and Smithsonian-wide procedures for returning keys were contradictory and failed to ensure that all keys from departing employees were returned to the Locksmith Shop. Previous employee exit procedures directed staff to submit their keys to their Administrative Officers. Administrative Officers were not instructed to return keys to the Security Managers; however, OPS procedures directed Security Managers to return keys to the Locksmith. Departments thus kept keys and redistributed them without the knowledge of either the Security Managers or the Locksmith.

- According to OPS management, training on and distribution of security system reports were delayed until new training facilities were constructed at the Institution's Pennsy Drive complex. Eventually, OPS distributed reports without training Security Managers on how to use the reports. Although reports were

discussed during some staff meetings, there was also little or no follow-up by TSD to determine the effectiveness of the reports.

- The security system at Garber monitors security events at four other Smithsonian facilities, resulting in cumbersome and lengthy reports of system activity. For example, a single Event Report for the week of March 21, 2009 was over 1,500 pages long.

Inadequate security in collection areas exposes NASM to an increased risk of theft, loss, or damage to objects. Inadequate control over keys reduces the effectiveness of locked doors as security devices, compromising physical access controls for secure areas. An inaccurate Key Holder List prevents the Smithsonian from knowing who has access to collection areas. In addition, ineffective and illogically formatted security system reports inhibit management from effectively managing operations and identifying opportunities to improve system operations.

Recommendations

To strengthen physical controls over access to NASM collections storage areas, we recommend that the Director, OPS:

4. Follow Technical Security Division policies and procedures and ensure that inspections of high-security areas are conducted quarterly and the resulting reports reviewed by the Technical Security Division.

5. Revise procedures to require that inspections validate the accuracy of alarm location information displayed on the security system monitors and reported on the Alarm Activity Reports.

6. Re-emphasize OPS requirements for security managers to review Key Holder List information semiannually, verify its accuracy and take appropriate corrective actions.

7. Implement procedures that require updating of Key Holder data when keys are issued to employees.

8. Improve security system reports that monitor activity and identify discrepancies at NASM facilities.

9. Provide training to Security Managers on how to produce and interpret reports from the security systems and ensure that Security Managers alert TSD to system problems.

We also recommend that the Director, OPS and the Director, OC:

10. Revise exit clearance procedures to ensure that all exiting employees return keys to the appropriate Security Managers.

NASM Staff do not Follow Inventory Plans

Presidential Medal of Freedom, 1968, James Webb, in storage at Garber facility

As noted in our audit of NMNH and ***Concern at the Core***, lack of compliance with inventory plans appears to be an ongoing problem throughout the Institution. We noted in our earlier audit that NMNH had not maintained accurate inventory records of all its collections objects, which made it difficult to account for, identify, and locate specimens and objects for research and exhibition. Also, museum staff had not performed cyclical inventory reviews as required by their own department inventory policies; updated inventory records to reclassify species name changes or to identify locations to where objects had been moved; or converted inventory records to a common format. Finally, inventory counts had showed a number of missing and misplaced objects.

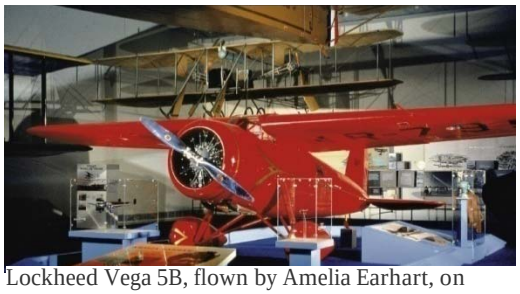
At NASM, similarly, staff have not conducted cyclical inventory reviews as required by the NASM Cyclical Inventory Plan. Routine inventory counts are a customary practice to confirm that all collection objects captured in an organization's inventory records are, in fact, on hand. Though NASM staff did not conduct the required inventory reviews, we were able through our testing to confirm that they could account for most of the collection objects in our random sample of 366 objects. We confirmed that 360 of these objects were on hand and accounted for. The remaining 6 objects were inaccessible because they were either installed in other objects on display (and could not be viewed), in a construction zone, or reported as missing from a prior theft.[9]

That NASM was able to account for all of these items is the result, in our opinion, of a number of unusual recent events. First, NASM staff moved a significant number of objects in preparing exhibits for the opening of the Hazy Center in 2003. In moving objects to Hazy, NASM took care to ensure that object locations were updated. Second, in response to recent thefts of collection objects, NASM staff conducted inventories of storage areas to identify additional missing objects. Any missing objects prompted adjustments to the inventory records. Lastly, as part of NASM's "Preservation, Preventative Care, and Re-housing for the Spacesuit and Aeronautic Flight Material Collections" project, over 4,400 objects were inventoried and re-housed from four different storage areas.

Although NASM staff accounted for nearly all the items tested in our sample, we believe they need to continuously emphasize collections accountability through the implementation of all the inventory control procedures required by their policies.

[9] This object was suspected stolen as part of a significant theft over a decade ago of valuable objects from secure storage; however, the records were not updated to show the object as "missing."

SD 600 and the corresponding ***Implementation Manual*** state that each unit must implement a continuous inventory system for (1) conducting, supervising, and approving cyclical inventories and reconciliation of collection records; (2) implementing a written cyclical inventory plan that is reviewed by all individuals who will conduct the inventory and approved by the museum director; and (3) ensuring separation of duties and implementation of other internal controls to prevent the unauthorized removal of collection objects. In addition, NASM's ***Cyclical Inventory Plan*** requires that two types of inventories be conducted in alternating fiscal years: (1) a complete inventory of the easily portable and high-value objects stored in the two Curatorial division secure storage rooms, and (2) a biennial inventory of a randomly selected sample of 0.5% of the accessioned collection. The Plan requires the NASM Registrar to analyze the results of the inventory and prepare a report for distribution to the NASM Director and Smithsonian Institution National Collections Coordinator.


Lockheed Vega 5B, flown by Amelia Earhart, on display at NASM Mall Museum

NASM Staff has not Conducted Cyclical Inventories

NASM staff reported to us that they conducted inventories required by ***SD 600*** and the NASM Inventory Plan, but could provide no documentation of the results of these inventories. NASM's Inventory Plan requires that the Chief of the Collections Division submit the final inventory results to both the NASM Director and the National Collections Coordinator. However, the failure to perform the required cyclical inventories and document any other inventories of the collection prompted no reaction from NASM management or the National Collections Coordinator.

* * * *

NASM was not conducting cyclical inventories for the following reasons:

- According to NASM management, the lack of adequate staff in the collections division has adversely affected NASM's ability to conduct and document inventories according to its Inventory Plan. (We note that, with the assistance of NASM Collections Processing staff, the audit team conducted an inventory of 366 randomly selected objects in approximately 24 hours spread over a seven-day period.)

- There was poor oversight of the inventory process. NASM senior management did not ensure that the inventories were conducted. In addition, the National Collections Coordinator lacks the authority to require that the museums conduct and report the results of inventories and thus could not compel NASM officials to perform these required inventory counts.

- NASM staff stated that although they had not completed the scheduled cyclical inventories, they had completed inventories of specific areas and collections (for other purposes) that accounted for a larger portion of the collection than if they had done the cyclical inventory. NASM staff believed that these inventories served as substitutes for the required cyclical inventories that were not being conducted.

By not conducting or documenting cyclical inventories, NASM has not exercised adequate control over the collection. NASM cannot rely on special review projects as a long-term substitute for ongoing inventory control procedures. To ensure sustained attention to safeguarding its collections, NASM officials need to return to the routine practices put forth in its policies.

Recommendation

To strengthen inventory controls, we recommend that the Director, NASM:

11. Ensure that staff conduct cyclical inventories and distribute the results according to the NASM Cyclical Inventory Plan.

Inventory Records Are Incomplete

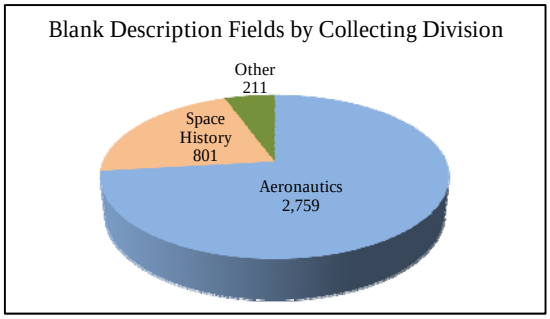
NASM staff did not maintain complete inventory records. We found that some collection records did not contain key identifying information such as object description and location. The primary cause for having incomplete object records was insufficient emphasis by museum management on complete recordkeeping. Objects with incomplete records are more vulnerable to loss or theft because identifying information, necessary to track them, is missing.

The ***SD 600 Implementation Manual*** requires that all collecting units create and maintain accurate and current inventory records that will identify, locate, and give an account of each object's condition to ensure maximum accessibility consistent with its security. NASM's ***Collections Management Policy (CMP)*** states that collection records maintained by the Office of the Registrar should be accurate and complete, which requires close coordination and cooperation among the registrar staff, the other units within the Collections Division, and the curatorial staff.

Incomplete Object Inventory Records

NASM did not have complete inventory records for all objects in the collection. NASM utilizes "The Museum System" (TMS) as its centralized electronic collections information system. We found the following examples of incomplete records in our review of the TMS database:

- Of the 56,717 records in TMS, approximately 6 percent (3,771 of 56,717) had a blank description field. Of the 3,771 incomplete records, 2,759 (or 73 percent) were for objects in the Aeronautics Division collection. Of the remaining 1,012 objects, 801 were from Space History and 211 were primarily from the Art collection ("Other").



- 389 objects believed to be missing were not recorded in TMS as missing; instead, the location field was left blank.

* * * *

We identified the following causes for NASM's collection records being incomplete:

- Performance plans for Aeronautics curators and museum specialists did not include specific, measurable goals for completing object records. According to NASM management, individual departments have been allowed to determine what goals to include in performance plans, as long as progress was made on completing the records. We note that performance plans for Space history staff did include specific goals related to completing object records.

- Although NASM registrars have identified incomplete records and periodically remind curatorial staff to address un-accessioned records, they have no authority to require the curators to complete object records.

- NASM Collections Division staff is responsible for updating the location fields for TMS records. According to NASM staff, many of these records were converted to the TMS database without location data. NASM staff hopes to locate objects within the collection when they conduct inventories.

The errors in the TMS database leave collections objects more vulnerable to loss or theft. In addition, incomplete records could adversely affect NASM's opportunity to fully use the objects for research, education, and exhibition purposes because museum staff may have difficulty locating and identifying the objects.

Recommendations

To strengthen inventory controls to ensure that records are complete, we recommend that the Director, NASM:

12. Add specific, measurable goals for completing object records to the performance plans for Aeronautics curators and museum specialists.

13. Require registrars to provide quarterly lists of incomplete records to the Space History and Aeronautics Division Chairs.

14. Based on the results of completed inventories, direct the Collections Division and Curatorial staffs to develop a follow-up plan to locate missing objects and update the inventory records accordingly.

Conflicting Duties

A traditional control technique in inventory management is to separate the responsibilities for managing objects and maintaining object records. Separating these duties minimizes the risk of records being adjusted to mask theft or loss. ***SD 600*** states that collection units must ensure adequate separation of duties and other internal

controls to minimize the possible unauthorized removal of collection items and corresponding records. ***The Implementation Manual*** further explains that there may be different levels of separation based on the value of the collections; while high-value collections may need full separation of duties, other collections may only need an audit trail to track changes. It also states that where separation of duties is not possible, other compensating controls should be implemented to minimize any risks.

NASM is not ensuring that there is an adequate separation of duties between employees with access to the collection and access to object records. We identified two employees with physical access to all but one collection storage area who also had access levels in TMS that allowed them to change locations, edit object information and delete the audit trail of activity for the record. According to NASM management, the departure of the former System Administrator resulted in both a registrar and conservation staff member assuming TMS System Administrator level access and responsibilities. Their daily responsibilities require that they also have unrestricted access to most of the collection.

This condition was a result of insufficient collections staff and resources. Without proper separation of duties it would be possible for an employee to take an object from the collection and delete all records regarding the object, including the audit trail of the object.

Recommendation

To prevent staff from having unrestricted access to both objects and object records, we recommend that the Director, NASM:

15. Assign a TMS System Administrator who does not have physical access to the collections.

MANAGEMENT RESPONSE

The Directors of the Office of Protection Services and of the National Air and Space Museum, as well as the Comptroller of the Smithsonian, provided consolidated, formal written comments to our November 23, 2009 draft report. In their February 17, 2010 comments they generally concurred, in whole or in part, with 13 of our 15 recommendations. They acknowledged that security of the collections did not meet OPS standards and that security controls were inadequate. They agreed that inventory plans were not being followed and that inventory records were incomplete.

Below, we summarize their comments and then offer our responses to those comments.

Overall Comments: Risk to Collections

Management emphasized that it works diligently to improve collections security. According to OPS, it continuously monitors security risks and responds appropriately to remedy unacceptable risks.

Despite these assurances, OPS officials acknowledged their awareness of the security deficiencies within NASM collections and conceded that nearly all collections storage areas within the Smithsonian do not meet current OPS security standards. OPS noted that "much of SI collections storage does not meet other facility requirements such as adequate space, mechanical systems, fire systems, etc." OPS characterized these deficiencies as "widespread and wide-ranging."

To remedy the known security and facilities deficiencies would require multiple, "stand alone" upgrade projects, an approach the Smithsonian characterized as "fruitless, inefficient, and irresponsible." OFEO and OPS stated that such projects would burden the Smithsonian Capital program, potentially harm operations and collections, and would be a wasteful diversion of resources. OFEO stated that it would be more efficient to perform security upgrades in conjunction with other storage facility upgrades and pointed out that the Institution lacks a long-term collections storage plan. OFEO and OPS expressed confidence in their decisions not to remediate security deficiencies in NASM storage facilities because they believe that the storage facilities are relatively safe and no NASM collections are at risk.

Physical Security Did Not Meet OPS Standards

OPS asserted that it conducts informal security assessments at NASM storage facilities and that additional security assessments are unnecessary. OPS agreed that the results of these assessments were not properly documented and plans to develop a formalized assessment program and tool by June 30, 2011. OPS did not believe that a higher priority should be placed on budgeting for NASM facilities and did not concur with the second recommendation, which it interpreted as calling for putting NASM's security needs above other competing priorities within the Smithsonian. OPS stated that they already prioritize high-security areas in its development of projects and requests for funding. By June 30, 2011, OPS will finalize and issue the ***OPS Collections Management Security Standards***.

Improperly Functioning Security Controls

OPS Management did not believe that it was provided adequate time to respond to reports of inoperable or malfunctioning devices and stated that it had not been made aware of security-related issues identified during the audit. OPS also asserted that OIG did not provide detailed information regarding the specific locations of inoperable and malfunctioning devices until September 30, 2009.

OPS also stated that OIG used outdated OPS standards to assess security; that OIG's characterizations were "grossly misleading;" and that security devices that indicated the wrong location for breaches were not functioning improperly. In addition, OPS asserted that such "system discrepancies did not result in a higher risk to the security of the collections."

Although management did not concur with the recommendation to improve quarterly inspections of high-security areas, it agreed to revise procedures to validate the accuracy of alarm location information. OPS did not provide an implementation date.

By June 30, 2010, OPS will update key holder data where appropriate for NASM facilities and will develop a long-term plan and schedule to identify where facility Key Holder Lists should be updated or where the facilities should be completely or partially re-keyed. By September 30, 2010, OPS will begin to review Key Holder Lists for accuracy. OPS agreed to improve security system reports and train Security Managers to interpret these reports by March 30, 2011. By June 30, 2011, the OPS and OC Directors will also develop new exit clearance procedures for the on-line exit clearance process.

Inventory Control

The NASM Director concurred with all five recommendations directed to him. By January 31, 2010, NASM formulated metrics for measurable goals for completing records and included these metrics in the FY 2010 Aeronautics Division performance plans. The NASM Office of the Registrar will distribute quarterly lists of incomplete records to the Aeronautics and Space History Divisions by March 31, 2010. The Collections Division and Curatorial staff will develop a plan to identify missing objects and update inventory records. By June 30, 2010, NASM will conduct its FY2010 inventory and will distribute the results according to its Cyclical Inventory Plan. NASM is researching several options for having a TMS System Administrator who does not have physical access to the collections. However, according to NASM management, all options require additional funding and, therefore, NASM does not provide an implementation date.
We include the full text of management's response as Appendix B.

OFFICE OF THE INSPECTOR GENERAL COMMENTS

<u>Overall Comments: Risk to Collections</u>

We recognize the importance that OFEO and OPS place on collections storage security, as well as their efforts to achieve improvements in this area. We acknowledge that these efforts align with the strategies and objectives in the Smithsonian's Strategic Plan to "improve the quality of collections preservation, storage space, management, information content, and physical and electronic access."

However, we disagree with OFEO and OPS's assertion that the collections are not at risk. [redacted] (b) (2) [redacted] Missing or malfunctioning security devices helped create the environment that allowed for unauthorized access and made the theft difficult to pursue.

We do agree with OPS's implicit assertion that the security of the collections depends on more than security devices and procedures; it also requires adequate structures and facilities systems. The Institution's failures in this regard were starkly illustrated by the February 10, 2010 collapse of Building 21 at Garber, which housed approximately 2,000 objects and works of art related to aviation and space travel. The snow and extreme wind conditions associated with an unprecedented blizzard that week caused the building to buckle. We inspected the exterior of the damaged building but were unable to enter to assess the state of the collections. We consulted with NASM staff, who confirmed that some collections contained in the building were damaged, but they do not yet know the extent of the damage. We learned that the building is not repairable and eventually will have to be demolished. In the interim, the Smithsonian is working with a contractor to stabilize the building adequately so that it may salvage the contents.

We agree that a strategic, Institution-wide plan for collections storage would be a prudent and efficient approach to managing collections security and facilities. But the lack of such a plan cannot justify avoiding pressing short-term security and facilities issues. We question the Smithsonian's policy of refusing to remedy known storage facilities deficiencies on the grounds that to act would be fruitless, inefficient, and irresponsible. We believe that a balanced approach to assessing collections storage risk, one that weighs long-term goals against immediate shortcomings, is critical to safeguarding collections.

OPS pointed to compensating controls which they believe mitigated the risks to the collections created by missing or malfunctioning security devices. That is, [redacted] (b) (2) [redacted] We strongly disagree. [redacted] (b) (2) [redacted] We question OPS's reliance on compensating controls, rather than primary controls, to prevent and detect improper access.

Physical Security Did Not Meet OPS Standards

We reaffirm our recommendation that OPS develop a plan with a timetable to conduct formal security assessments of the NASM, Hazy, and Garber facilities. We disagree with OPS's assertion that its informal, but poorly documented, security assessments were adequate.

During the audit, we saw no evidence that OPS conducted or documented any security assessments since a partial review of Garber in 2006. We followed up with OPS officials to understand the nature of the security assessments they claim to have conducted. OPS officials informed us that these assessments consisted of nothing more than staff being generally aware of the state of security at NASM and making mental notes of problems they observed. OPS did not demonstrate that it: followed a timetable for its assessments; developed related assessment steps; identified skills or training requirements for individuals responsible for conducting its assessments; had a policy for documenting the results and distributing them to stakeholders; or had a mechanism to assign accountability for follow up or to track the results of corrective actions, all fundamental components of a security risk assessment. It is difficult to understand how OPS can rely on this informal assessment approach to manage security or provide meaningful information to decision-makers on such matters as resource needs.

We believe that OPS misinterpreted our second recommendation. There is nothing in the recommendation, implicit or explicit, that calls for OPS to place a higher priority on NASM, Hazy, and Garber high-security areas than on other areas in the Institution. The recommendation simply calls for OPS to construct its budget requests based on risk. We made our position clear in our January 27, 2010 meeting with OPS and OFEO management and are therefore puzzled at their final response. We will accept the language in their response as a concurrence with the recommendation.

Improperly Functioning Security Controls

At all times we communicated the results of our testing immediately to the OPS officials on site designated by OPS as our contacts for the audit. We provided OPS officials with sufficient information for them to act throughout the course of the audit, as the following chronology clearly shows:

- **4/17/09** – We conducted our first round of testing with the TSD System Administration Section Supervisor present. We identified several security deficiencies. The TSD Supervisor agreed these deficiencies should be corrected and took notes to make corrective actions.
- **5/6/09** – We conducted our first test of a high-security area. We notified a Security Manager of the deficiencies and he immediately submitted a work order to TSD for repairs.
- **6/2/09** – We met with NASM and OPS staff to discuss security issues and the results of our testing. OPS representatives at the meeting included the TSD System Administration Section Supervisor, a TSD System Administrator, and a Security Manager.
- **6/18/09 and 6/19/09** – On June 18 we re-tested a repaired security device with the assistance of a Security Manager. The security device failed and the Security Manager submitted a work order for repairs. We returned on June 19 to re-test

the device with the assistance of a TSD System Administrator. The TSD System Administrator could not explain why the device had not worked properly the previous day.

- 7/10/09 – We met with the TSD System Administration Section Supervisor at our offices. We discussed our tentative findings on the failed and missing security devices.
- 7/20/09 – We met with NASM and OPS staff to discuss security concerns. OPS representatives included the TSD System Administration Section Supervisor, a TSD System Administrator, a Security Manager and an Assistant Security Manager. We discussed our tentative findings on the failed and missing security devices.
- 7/30/09 – We met with the TSD Associate Director and TSD System Administration Section Supervisor. In addition to discussing the budgeting and security improvement process, we discussed our tentative findings on the failed and missing security devices.
- 8/18/09 – A TSD System Administrator accompanied us during our testing of high-security areas. After we completed the testing we met with the TSD administrator and NASM staff to summarize the results.
- 9/18/09 – We issued a confidential memorandum to the Directors of OPS and NASM detailing the security deficiencies identified during our audit.
- 9/30/09 – TSD staff provided a report on corrective actions OPS had taken on several of the security devices we had identified in our September 18 memorandum, showing that OPS completed most of the repairs prior to September 30, 2009.

That OPS corrected several of the shortcomings we identified before our meeting on September 30 also belies the assertion that we failed to provide OPS sufficient notice. Indeed, we were pleased by OPS's prompt, if initially incomplete, responses.

OPS management's claim that we did not notify them of these problems indicates a communications problem within the organization. It appears that senior OPS officials were not aware of the results of our testing nor their subordinates' corrective actions. We did not audit the flow of communications of our audit test results through to senior OPS officials. As such we cannot account for the basis of the Director's lack of awareness. In view of the functional role OPS plays in safeguarding Smithsonian facilities and collections, the communications breakdown concerns us. We will of course seek to advise the Director of OPS on all such matters in future audits.

OPS' assertion that we used obsolete criteria to identify security devices that should have been installed in high-security collection storage areas is also incorrect. As we clearly stated in the report, we used both sets of standards available during the audit and concluded that collection storage areas did not meet either. And we are surprised that OPS emphasized the distinction between the old and new security standards, when it freely acknowledges that the Smithsonian does not comply with either. The emphasis on the change in security standards is additionally confusing in that OPS has no immediate plans to conduct assessments of these areas to bring the Institution into compliance with the most recent standards.

We also take issue with OPS's statement that we were "grossly misleading" in our reports of improperly functioning devices. As we stated in our report, [redacted] (b) (2) [redacted] Nowhere in the report do we generalize beyond what we examined.

OPS disagreed that security devices are functioning improperly when those devices indicate the wrong location for security breaches. OPS would prefer to describe the faulty devices as having "incorrect location descriptors in their programming." We maintain that devices that misdirect attention from the true location of access breaches fail their intended purpose and compromise security.

Lastly, OPS did not concur with our recommendation to follow its policy of conducting quarterly inspections of high-security areas. OPS responded that quarterly tests were unnecessary and an inefficient use of limited resources, and that semiannual inspections are sufficient. OPS has changed its policy to reflect the new schedule. OPS reasoned that the lack of security problems noted from prior security reviews support the decision to conduct reviews only twice a year. However, OPS's inspections failed to identify several security vulnerabilities, as noted in our audit. Therefore, we affirm our recommendation not to relax its inspection cycle until future inspection results demonstrate that less frequent testing is appropriate.

APPENDIX A. SCOPE AND METHODOLOGY

The objectives of this audit were to determine whether NASM's physical security controls were adequate to safeguard the collections and whether inventory controls were in place and adequately working to ensure the collections are properly accounted for in compliance with collections management policies and procedures.

We reviewed previous reports of security and inventory control measures safeguarding the Smithsonian's collections. We also reviewed the Smithsonian's policies, procedures, and other documents related to collections security and inventory controls.

Physical Security

To assess physical security controls at NASM, we toured the collections storage areas of NASM's Mall Museum; the Steven F. Udvar-Hazy Center in Chantilly, Virginia; and the Paul E. Garber Preservation, Restoration, and Storage Facility in Suitland, Maryland to inspect and test security devices. We opened secured doors to determine whether alarms were working properly and to determine the response of security officers. We also observed alarm activity from the OPS control rooms at all three facilities. We accompanied OPS Technical Security staff to various buildings to test the functioning of card reader security devices at the Garber Facility.

We interviewed OPS management and staff to determine physical security policies and procedures. We met with NASM collections management officials to discuss their concerns with physical security, communications with OPS, and internal museum policies and procedures regarding access to collections.

We assessed OC's exit clearance procedures and discussed our observations with OC management.

Inventory Controls

We evaluated the collections management controls and procedures at the museum and performed tests of its records to identify procedural strengths and weaknesses. We reviewed the adequacy of controls over the collections inventory system. We verified compliance with Smithsonian procedures for safeguarding the Museum's collections. We interviewed management and staff registrars and museum specialists at both the Museum's Washington, D.C. Mall location and Garber Facility.

We obtained a copy of the Museum's collections information system (The Museum System or TMS) and conducted a spot check of objects based on a statistical sample from the records. We selected a random sample of 366 objects, or 0.75% of the NASM collection, using a 95% confidence level and an expected error and margin of error of 4% and 2%, respectively.[10] We observed and reviewed the results of inventories conducted by

[10] To pick our random sample, we assigned all accessioned objects, excluding unassigned records, a random number in Microsoft Excel. We excluded missing objects, incoming and outgoing loans, items with locations recorded as "other" or "unknown," and objects located at the Aerospace Maintenance and Regeneration Center in Tucson, Arizona. We also excluded objects stored in the Space History and Aeronautics collection secure-storage areas at the Mall Museum because NASM staff inventoried these collections during the audit.

staff during the audit period. We also performed analytical reviews of the data in TMS to assess record completeness and identify backlogs of temporary objects.

We conducted this performance audit in Washington, D.C., from February through November, 2009, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Smithsonian Institution

Memo

Office of Protection Services

Date February 12, 2010

To A. Sprightley Ryan, Inspector General

cc Bruce Kendall, Director, Office of Facilities Engineering and Operations
Alison McNally, Undersecretary for Finance and Administration
Alice Maroni, Chief Financial Officer
William Tompkins, National Collections Coordinator
Peter Jakab, Associate Director, Collections and Curatorial Affairs Department, National Air and Space Museum
Elizabeth Garcia, Chief, Collections Division, National Air and Space Museum
Doug Hall, Associate Director, Office of Protection Services

From James J. McLaughlin, Director, Office of Protection Services
John R. Dailey, Director, National Air and Space Museum
Andrew J. Zino, Comptroller

Subject Response to Inspector General Draft Report on the Audit of Physical Security and Inventory Control Measures to Safeguard the National Collections at the National Air and Space Museum, Number A-09-04.

This response is submitted on behalf of the Office of Protection Services (OPS), the National Air and Space Museum (NASM), and the Office of the Comptroller (OC).

We appreciate the hard work of the Office of the Inspector General (OIG) auditors in this complicated review.

We accept many of the findings of the audit. However, it is important to respond up-front that although we work diligently to make continuous improvements to the overall collections security throughout the Institution, SI collections are not at risk, and we are continually checking and monitoring to ensure this fact. We take our responsibility very seriously to evaluate security risks and respond appropriately to remedy those deemed unacceptable.

OIG indicated several times in the report that that "The Smithsonian had not installed required security devices." They also indicated that the Smithsonian Institution Capital Planning Board ultimately makes the decision on most security upgrades. While true, we wish to elaborate on the process by which this happens. By far, the majority of security-related systems, equipment, and devices are installed/constructed through the Facilities Capital Program, either during the construction of new facilities, the upgrade or renovation of existing facilities, or occasionally through large, facility wide security upgrade projects. OPS only requests these large security projects when there is no near-term compatible, existing renovation project in the Capital Program where a facility's security could be logically upgraded. We generally bundle many small security needs to create large projects for the OPS portion of the Facilities Capital Program if a major facility renovation is not planned. OPS rarely requests small stand-alone security projects

Capital Gallery, Suite 4100
600 Maryland Avenue SW
Washington, DC 20024, MRC 504
202.633.5650 Telephone
202.633.5617 Fax

unless there is compelling need (e.g., unacceptably high security risk) because of the inefficiency of managing (administratively and financially) hundreds of small security projects. This strategy, and OPS' role in security upgrades or improvements for collections storage areas is the same. In our efforts to improve security throughout all of SI, OPS will continue to make the case for security improvement projects where warranted, but the funding decisions rest with the Capital Planning Board and SI leadership.

As they indicate in their report, OIG used the obsolete *Protective Design Standards for Technical Security (Revision 8, dated December 27, 2004)* as an audit baseline. This document was retired during the OIG audit and replaced with the *SI Security Design Criteria (March 2009)*. We realize now that this change in criteria may have been confusing. Regardless, it is important to realize that both documents were intended to be applied in the same manner. Similar to building codes for life-safety, accessibility and mechanical/electrical/plumbing systems, we primarily use these as objective standards to guide future new construction, renovations and revitalization projects and seek to apply retroactively only those stand-alone security improvements that are warranted by risk analysis and evaluation. The majority of security systems and elements are implemented and funded through major revitalization projects (which may include an occasional large security upgrade project), similar to most other code compliance issues.

We feel the OIG statement that "some security controls were frequently malfunctioning or inoperable" is an over-generalization. This terminology exaggerates the severity and extent of the system deficiencies within SI's security systems. As explained in much greater detail in Attachment A, the vast majority of these system discrepancies did not result in a higher risk to the security of the collections they were intended to secure.

We appreciate OIG's recognition of OPS' attempts to improve security policy and procedures by their recommendation to finalize the OPS-drafted *Collections Management Security Standards*. We will work more closely with Museum Directors and the National Collections Program to ensure that their collections are not inadvertently moved to improperly secured, non-designated collections areas, and we will develop policies that affix responsibilities and procedures to implement them.

In addition to the general comments above, OPS also offers some specific additional clarification to the audit findings:

<u>OIG Finding: Security of the Collections Does Not Meet OPS Standards</u>

OPS Response: Concur, with clarification.

As OIG indicates, OPS is aware of security deficiencies within NASM collections storage areas. Furthermore, OPS is also well aware that nearly all collections storage areas within SI do not meet current objective OPS security standards. OIG's planned audit of NMAH collections storage will yield similar findings although we feel that they are secure.

Additionally, much of SI collections storage also does not meet other facility requirements such as adequate space, mechanical systems, fire systems, etc. Because of these deficiencies, OPS has not pursued funding for potentially hundreds of small stand-alone security upgrade projects (like NASM collections storage). OPS feels that addressing widespread and wide-ranging deficiencies through piecemeal efforts is not only fruitless (because of limited funding), but inefficient and irresponsible.

Absent a pan-institutional, long-term collections storage facility planning effort, OFEO and OPS currently feel that renovating collections storage, including security, is most efficiently done in conjunction with overall facility renovations and upgrades rather than in hundreds of stand-alone collections storage upgrade projects. Generally, except in the case of very high risk collections, OPS follows the strategy of implementing our objective security standards, to include collections storage, during other and greater renovation and construction projects that are part of the SI Facilities Capital Program. Even if greater amounts of funding were available, without a clear long-term plan to improve collections storage, OPS feels it would be irresponsible to do stand-alone security projects because we are relatively secure and:

1) Adding hundreds of collections storage security upgrade projects (for all SI collection storage security deficiencies) would further overburden the SI Capital Program.
2) It is more efficient (from both an administrative as well as a funding perspective) to perform security upgrades in conjunction with other much needed collection storage facility upgrades.
3) It is upsetting to facilities operations and potentially harmful to collections to stage multiple upgrade projects. One single multi-focused upgrade would minimize the impact on museum operations and reduce the risk of damage (movement or protection from construction) to collections.
4) A long-term collections storage plan, and the supporting research, may prove that it is more efficient or appropriate to fund or to identify new facilities rather than to renovate existing facilities. Without that information and overarching guidance, upgrades (including security) to existing collections storage may be an unnecessary and wasteful diversion of resources.

OIG Recommendation 1: Conduct security assessments of the NASM, Hazy, and Garber facilities, document the results, and develop a plan, in the context of overall Smithsonian funding priorities, to acquire missing security devices.

OPS Response: OPS partially concurs with this recommendation.

OPS has conducted and will continue to conduct security assessments in general. As a result of these assessments at NASM, OPS has developed a long list of new requirements and upgrades (to include collections storage) and will begin design of a large security project this fiscal year. Currently, there is funding on the Capital Program in FY 2015 for this project and we do not feel it warrants more immediate action. OPS has similar, smaller lists of needs for Garber and Hazy, but will await renovation (or replacement) of Garber facilities to execute any additional security requirements.

In essence, security assessments have been performed for these facilities, and any additional assessments are unnecessary. However, OPS agrees with OIG that we have not properly documented the results of these assessments. We also agree that the assessment program is not as “formal” as it should be. OPS has been aware of this deficiency and

Capital Gallery, Suite 4100
600 Maryland Avenue SW
Washington, DC 20024, MRC 504
202.633.5650 Telephone
202.633.5617 Fax

formerly identified it as an area for improvement in the *Smithsonian Institution Response to Board of Regents' Governance, Recommendation # 23.*

OPS intends to develop a more formalized assessment program and assessment software tool (to facilitate the assessments and record the results) that would be based on Federal criteria, the SI Security Design Criteria, and OPS policies and procedures.

Estimated Program Completion and software tool development: June 30, 2011

OIG Recommendation 2: Ensure that OPS budget requests reflect the priorities identified in the Security Assessment, placing higher priority on installations of required security devices in high-security areas.

OPS Response: OPS does not concur with this recommendation.

OPS strongly disagrees with any recommendation to place higher priority on NASM, Hazy, and Garber than on the rest of the Institution; no risk-based information was provided to justify such a preference. OPS believes that, within the context of the entire Institution, NASM collections security needs have been prioritized appropriately.

If this is not OIG's intent by this recommendation, then it would appear that OIG simply wants OPS to prioritize high security areas in our creation of projects and requests for funding. OPS already does this appropriately and consistently through the development of our few stand-alone security projects.

OIG Recommendation 3: Finalize and issue the *OPS Collections Management Security Standards.*

OPS Response: OPS concurs with this recommendation.

OPS will work with the National Collections Coordinator to develop a working group to review the *Collections Management Security Standards,* gain consensus, and publish it in the most appropriate manner that will ensure its compliance.

Estimated Completion: June 2011.

OIG Finding: Improperly Functioning Security Controls: *Improperly Functioning Security Devices*

OPS Response: OPS does not concur with this finding.

Although OPS agrees that some security devices had incorrect (or partially incorrect) location descriptors in their programming (or labeling), all but one device that the OIG tested was operating properly, and in most cases those with incorrect location descriptors did not compromise the security of those areas. The OIG statement that "many" security devices were "often malfunctioning" is grossly misleading. OIG tested [redacted] (b) (2) throughout the NASM Mall museum and Garber facilities. Nearly [redacted] (b) (2) exist between these facilities. At the request of OIG, OPS has provided our detailed response and clarifications in a separate Attachment A.

Capital Gallery, Suite 4100
600 Maryland Avenue SW
Washington, DC 20024, MRC 504
202.633.5650 Telephone
202.633.5617 Fax

OIG issued a high level discussion of the results of their testing and inspections in a document separate from the main audit report; *Management Advisory on Security Issues at the National Air and Space Museum, No. M-09-04, dated September 18, 2009.* This was issued the same day as the original Discussion Draft of the report; September 18, 2009. However, OIG did not provide OPS with a copy of the detailed report backup (which identified specific locations of "inoperable" and "malfunctioning" devices) until September 30, 2009. In several locations of this Management Advisory, the report states that OIG had given (presumably before September 18) their "detailed" findings of problems and issues to OPS, and that OPS had not acted on these findings. Obviously, it was impossible for OPS management to act upon these issues without being notified by the OIG that they existed. OIG seemed to recognize this, but to date OIG has not corrected this discrepancy within their Management Advisory. By not correcting the Management Advisory to clarify that OIG never issued the detailed findings, or to remove the sections that indicate OPS did not act on their findings, OIG gives the inaccurate impression of unresponsiveness by OPS.

In the future, when the OIG identifies security-related issues in the field while conducting audits , OPS would appreciate, in addition to informing the local security staff, that OIG provide the Director, OPS, with their findings in writing so that we may correct (and track) the issues, if valid, in the most efficient manner. We feel this is reasonable, particularly if OIG will continue to track and discuss OPS responsiveness in their reports.

OIG Finding: Improperly Functioning Security Controls: *Weak Control Over Keys*

OPS Response: OPS concurs with this finding.

OIG Finding: Improperly Functioning Security Controls: OPS Security Management System Needs Improvement

OPS Response: OPS concurs with this finding--with clarification.

The security management systems that monitor intrusion detection, access control, and CCTV at SI facilities are commercial off-the-shelf (COTS) products that are difficult to "improve." Changes to software must be made by the manufacturer; doing so without substantial funding (for those changes) is impossible. Additionally, any changes to well-tested COTS software comes with some inherent risk (possible glitches) if that change is implemented for a sole customer. Manufacturer testing is much more robust when conducted in concert with an upgrade or modification to a standard COTS product. Although there are occasional issues with OPS Security Management Software, most issues are not malfunctions but rather functions that are not as "user friendly" to OPS operations as we might prefer. In the case of the NASM [redacted] OPS will soon replace that system with a [redacted] to standardize our systems throughout SI and to provide a more OPS management-friendly system. We will also work to customize some of the reporting capabilities on the [redacted] to be more user friendly to OPS management. (b)(2) (b)(2) (b)(2)

We also wish to clarify a finding within the report:

> *"OPS only tested the security devices at the three NASM facilities semi-annually, rather than quarterly as required by the TSD High Security Area Inspection and Maintenance Program."*

Capital Gallery, Suite 4100
600 Maryland Avenue SW
Washington, DC 20024, MRC 504
202.633.5650 Telephone
202.633.5617 Fax

While this is true, OPS intentionally had not recently quarterly tested any high-security areas. After the start of this program and after the first several quarterly tests that OPS performed (throughout all of SI), we found the testing yielded no new information. Basically, OPS received the same results and felt that quarterly testing was an unnecessary and inefficient use of limited resources. We adjusted our policy to perform the testing only every six months. However, although we updated our testing schedule, we failed to update the *TSD High Security Area Inspection and Maintenance Program* procedure documentation. OPS has since amended the documentation.

OIG Recommendation 4: Follow Technical Security Division policies and procedures and ensure that inspections of high-security areas are conducted quarterly and the resulting reports reviewed by the Technical Security Division.

OPS Response: OPS does not concur with this recommendation.

As previously stated, OPS feels that bi-annual testing is adequate for the high-security testing program. We have now modified the *TSD High Security Area Inspection and Maintenance Program* procedure documentation to reflect this need; we are now in compliance with our own program. Because TSD manages the testing, they already review all program reports.

OIG Recommendation 5: Revise procedures to require that inspections validate the accuracy of alarm location information displayed on the security system monitors and reported on the Alarm Activity Reports.

OPS Response: OPS concurs with this recommendation.

This was a valuable recommendation within the report. OPS has already made the change to the testing procedures to validate the programming. Additionally, OPS will add another staff person to the testing procedure solely for this purpose.

OIG Recommendation 6: Re-emphasize OPS requirements for security managers to review Key Holder List information on a semi-annual basis, verify its accuracy and take appropriate corrective actions.

OPS Response: OPS concurs with this recommendation.

As the OIG correctly identified, OPS management staff had not performed regular audits and reviews on facility Key Holder Lists as required by OPS internal policy. Based upon OIG's valuable input, OPS has realized that several internal key and locksmith policies require improvement. Additionally, rather than serve merely as internal OPS policies, key control and management policies should be available for all SI staff such that they also realize their responsibilities in regard to key control and management.

Estimated Policy Completion and Publication: September 30, 2010

Based upon OIG's findings, OPS also will establish an internal audit and review function that will manage a calendar for assigning reviews (such as the Key Holder Lists). This

audit and review function will also include the performance of random audits and reviews to ensure compliance with this and other management review requirements.

Estimated Completion of Audit and Review Calendar and initiation of Audit and Review Program: September 30, 2010

OIG Recommendation 7: Implement procedures that require updating of Key Holder data when keys are issued to employees.

OPS Response: OPS concurs with this recommendation.

Based on the OIG findings, OPS has already begun to update Key Holder data, but this task will take considerable time at some SI facilities. OPS believes that it may be more productive to re-key at those facilities, rather than to update many years of obsolete data. OPS will develop a long-term plan and schedule to identify at which facilities Key Holder Lists should be updated or the facilities completely, or partially, re-keyed.

Estimated date for completion of schedule: June 30, 2010

OPS will incorporate proper Key Holder Data maintenance in the new policy referenced in our response to Recommendation 6.

OIG Recommendation 8: Improve security system reports that monitor activity and identify discrepancies at NASM facilities.

OPS Response: OPS concurs with this recommendation.

The issues identified within this audit for NASM can also be found at other SI facilities. Therefore, OPS must develop solutions that support the entire Institution. OPS will re-evaluate all security management system reports that should be generated, who will generate them, who should review them, and the frequency of the reviews. This will be a multi-step process and a project that requires participation from all sections and units of OPS. First, OPS will establish a clear list of the reports and the required frequency of review. This will include a review of the ease with which these reports can be generated and whether special software (e.g., (b) (2) is necessary to help generate these reports. The ability to generate "canned reports" will also be reviewed.

Estimated Completion of Report List: June 30, 2010

A small OPS working group will then gather to determine which staff should generate the reports and who should review them.

Estimated Completion of working group efforts: September 30, 2010

OPS will then develop an internal policy to document all report generation and review responsibilities.

Estimated Completion of Policy: December 30, 2010

After completion of the working groups efforts, OPS/TSD will visit each security unit and develop report shortcuts, canned reports, and install additional software (as needed) to ensure that each security unit has the capability to easily generate the required reports. Training will be performed as needed.

Estimated Completion of OPS/TSD efforts in response to this recommendation: March 30, 2011

Once this project is completed, the report generation and review process will be added to the new OPS Audit and Review function to ensure compliance.

OIG Recommendation 9: Provide training to Security Managers on how to produce and interpret reports from the security systems and ensure that Security Managers alert TSD to system problems.

OPS Response: OPS concurs with this recommendation—with clarification.

Depending upon the results of the working group identified in the OPS response to Recommendation 8, it may be determined that OPS Security Managers may not be the most appropriate staff to review all reports. However, OPS will provide training to all staff determined to generate and review the reports.

Estimated completion of training: March 30, 2011

For both the Director, OPS and the Director, OC:

OIG Recommendation 10: Revise exit clearance procedures to ensure that all exiting employees return keys to the appropriate Security Managers.

OPS and OC Response: OPS concurs with this recommendation--with clarification.

Prior to the OIG audit, OPS had begun working with OC to develop new exit clearance procedures (for keys and SI credentials) in conjunction with the new on-line exit clearance process that OC had developed. Based on the OIG's report, OPS will also update and publish new key control and management policies to indicate that all keys must be returned to the appropriate OPS office.

Estimated completion of exit clearance procedures: June 30, 2010

For the Director, NASM:

OIG Recommendation 11: Ensure that staff conducts inventories and distribute the results according to the NASM Cyclical Inventory Plan.

NASM Response: NASM concurs.

NASM concurs with the recommendation and has already begun complying by completing an inventory of the Aeronautics Division secure storage room, the Division of Space History secure storage room, and a random object inventory of more than 300 objects in 2009, and has scheduled the FY 2010 inventory.

Estimated completion of FY 2010 inventory: June 30, 2010

OIG Recommendation 12: Add specific, measurable goals for completing object records to the performance plans for Aeronautics curators and museum specialists.

NASM Response: NASM concurs.

The Aeronautics Division chairman has been directed by the Associate Director for Collections and Curatorial Affairs to formulate metrics for goals for completing object records. These metrics will be incorporated in the FY 2010 Aeronautics Division performance plans currently in preparation.

Estimated completion date: January 31, 2010.

OIG Recommendation 13: Require Registrar to provide quarterly lists of incomplete records to the Aeronautics Division and the Division of Space History.

NASM Response: NASM concurs.

This requirement will be placed in the Registrar's performance plan. NASM staff will develop appropriate database queries highlighting deficiencies in object records that will allow for quick checks of the current status of records.

Estimated completion date: The NASM Office of the Registrar expects to have such reporting available by the end of January 2010, and will begin distributing these reports by March 31, 2010.

OIG Recommendation 14: Based on the results of completed inventories, direct the Collections Division and Curatorial staffs to develop a follow-up plan to locate missing objects and update the inventory records accordingly.

NASM Response: NASM concurs.

Currently in development is a tracking spreadsheet that will act as a master list of missing objects. As cyclical inventories and the move of collections occur, unaccounted objects will be compared against this list for reconciliation and updated within the TMS database.

Capital Gallery, Suite 4100
600 Maryland Avenue SW
Washington, DC 20024, MRC 504
202.633.5650 Telephone
202.633.5617 Fax

Estimated completion date: Complete reconciliation will be an ongoing process, but the mechanism for reconciliation will be completed by March 31, 2010.

OIG Recommendation 15: Assign a TMS Systems Administrator who does not have physical access to the collections.

NASM Response: NASM concurs.

NASM is approaching this issue on a variety of fronts, with the ultimate goal of having an independent TMS System Administrator who does not have physical access to the collections. NASM has begun researching the possibility of splitting an FTE position between SI units using TMS, essentially allowing two units in need of a TMS administrator to have a half-time position each. When such a position could be in place is funding dependent. NASM currently has more than 25 vacant positions, approximately 10% of our workforce.

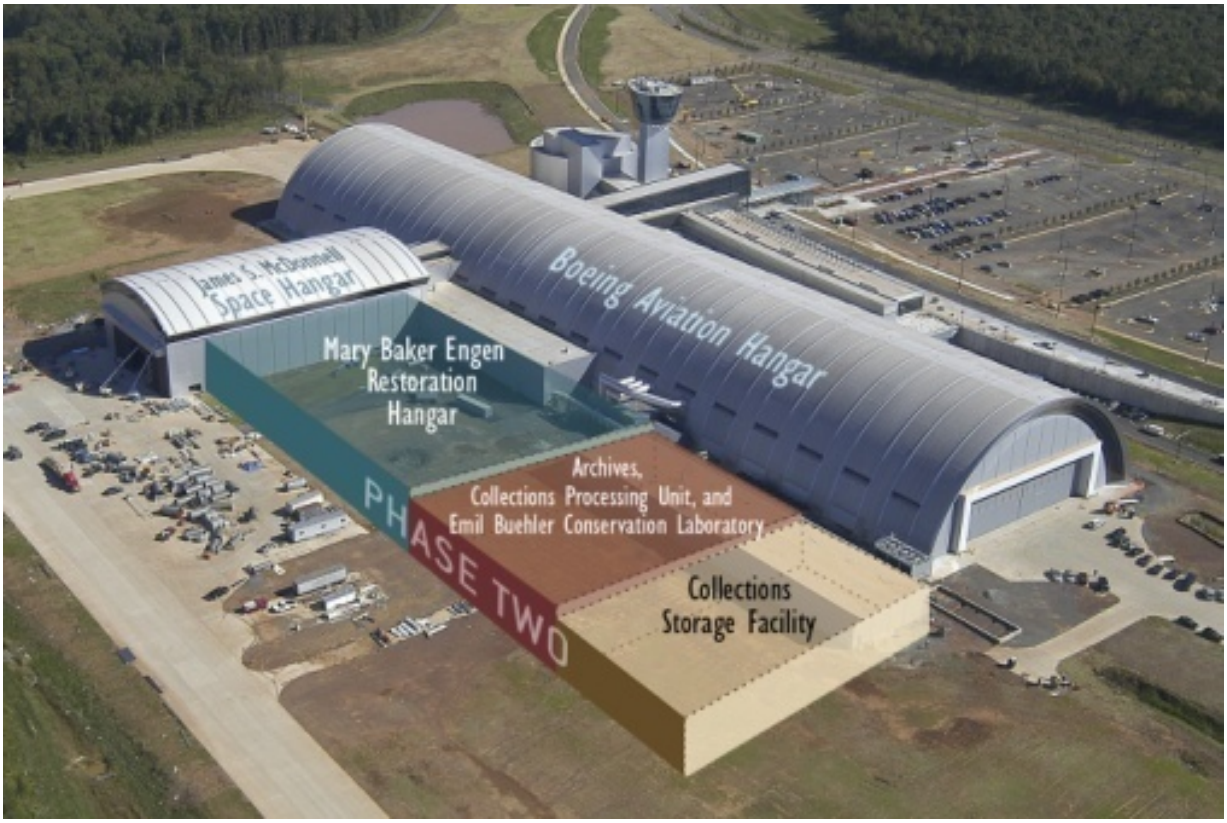
Anticipated completion date: This effort is funding-based and therefore undetermined.

Capital Gallery, Suite 4100
600 Maryland Avenue SW
Washington, DC 20024, MRC 504
202.633.5650 Telephone
202.633.5617 Fax

APPENDIX C. Images of NASM Facilities

National Air and Space Museum on the National Mall

Aerial View of the Paul E. Garber Storage Facility, Suitland, MD



Steven F. Udvar-Hazy Center in Chantilly, VA, with Phase II graphic rendering showing planned storage facility

"Shuttle Hangar" collection storage area on Dulles Airport property in Chantilly, VA; a C-130 aircraft is stored outside the hangar

APPENDIX D.

The following individuals from the Smithsonian Office of the Inspector General contributed to this report:

Daniel Devlin, Assistant Inspector General for Audits
Brian Lowe, Supervisory Auditor
Kimm A. Richards, Senior Analyst
Steven Townsend, Auditor
Brendan Phillips, Auditor