Description of document:	Closing documents associated with sixteen (16) National Archives and Records Administration (NARA) Inspector General (OIG) investigations, 2009-2014
Requested date:	31-January-2016
Released date:	02-November-2016
Posted date:	28-November-2016
Source of document:	National Archives and Records Administration Office of the OIG FOIA Request 8601 Adelphi Road, Room 1300 College Park, MD 20740 Fax: 301-837-3197

NATIONAL ARCHIVES

OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
8601 ADELPHI ROAD, COLLEGE PARK, MD 20740-6001
www.archives.gov/oig

November 2, 2016

Via email

Re: Request for OIG Investigations Information (NARA OIG FOIA 16-07)

This letter is in response to your email dated January 31, 2016 requesting "a copy of the Report of Investigation or Final Report or Closing Memo, etc." for a list of NARA OIG closed investigations. I have performed a search and have attached the Report of Investigation or closing memos. However, three of the requested investigations did not have any such documentation. Investigation 13-0003-I, while termed an investigation, was an administrative effort by the Office of Investigations to house various information on agency-wide information security violations in one location. As such, it has no report. Further, Investigation 14-0001-I shows the outreach completed by the Archival Recovery Team, and it has no final report. Investigation 14-0004-I was closed without any report as it was redundant with other investigations.

I am releasing the attached documents from the OIG files with information redacted mainly under FOIA Exemptions b(6) and b(7)(C) due to the privacy interests of the parties involved. Redactions pursuant to Exemptions b(6) and b(7)(C) included information that constituted a clearly unwarranted invasion of personal privacy and/or records compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. Some redactions, such as those detailing security response deficiencies at certain facilities, are redacted under Exemption b(7)(F) as they could reasonably be expected to endanger the life or physical safety of an individual. Please note all redactions on the disclosed pages were done by replacing information with a black line. In the interests of getting available information to you as fast as possible, I am disclosing this document immediately. If you wish for a redaction by redaction breakdown of exemptions, please contact me.

You have the right to administratively appeal those determinations by writing to the Archivist of the United States, National Archives and Records Administration, 8601 Adelphi Road, College Park, MD, 20740, within ninety (90) calendar days of the date of this letter. If you choose to appeal, your appeal letter and its envelope should be clearly marked "Freedom of Information Act Appeal," and you should explain why you believe NARA should release the withheld information.

If you would like to discuss our response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you may contact the OIG's FOIA Public Liaison, James Springs, for assistance at:

National Archives and Records Administration
Office of Inspector General
8601 Adelphi Road, Room 1300

College Park, MD 20740-6001
(301) 837-3018
james.springs@nara.gov

Further, some of the files also contained information from the US Department of Justice, Executive Office for United States Attorneys (EOUSA). Some of that information has been redacted under Exemption b(5) as inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency. Those redactions are done in a gray box, and are specifically marked as coming from the EOUSA. For those redactions from the EOUSA only, EOUSA does consider this the final action on the request. If you are not satisfied with this response to this request specifically about the marked EOUSA redactions, you may administratively appeal by writing to:

Director, Office of Information Policy (OIP)
United States Department of Justice, Suite 11050
1425 New York Avenue, NW, Washington, DC 20530-0001

You may also submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: https://foiaonline.regulations.gov/foia/action/public/home. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of this letter. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." You may contact their FOIA Public Liaison at 202-252-6020 for any further assistance and to discuss any aspect of your request.

If you are unable to resolve your FOIA dispute through the FOIA Public Liaison for the EOUSA or the NARA OIG, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman's office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road–OGIS
College Park, MD 20740-6001
ogis@nara.gov
ogis.archives.gov
202-741-5770 or 1-877-684-6448

Finally, in accordance with Department of Justice guidance, I would also like to notify you that Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification given to all our requesters and should not be taken as an indication excluded records do, or do not, exist.

If you have any questions, you may contact me at 301-837-1966 or john.simms@nara.gov. Thank you for contacting the NARA OIG.

Sincerely,

John Simms
Counsel to the Inspector General
Office of Inspector General
National Archives and Records Administration

NATIONAL ARCHIVES

OFFICE of INSPECTOR GENERAL

Date : September 30, 2013

Reply to : Matthew Elliott, Assistant Inspector General for Investigations

Subject : **Assessment of Researcher Registration at the National Archives and Records Administration (13-0014-I)**

To : Jay Bosanko, Chief Operating Officer, Office of Chief Operating Officer (C)

PURPOSE

The Office of Investigations (OI) performed a limited assessment of National Archives and Records Administration (NARA) procedures for issuing researcher cards and methods used to verify researcher identity. The OI also reviewed whether electronic databases are used to capture researcher data and track researcher access to NARA facilities. This report is informational and is meant to convey observations to management that may help NARA create an improved NARA-wide researcher registration system (RRS).

SCOPE

The OI generally assessed the current researcher registration procedures at Archives I and II, the National Archives at San Francisco (RW-SB), and the Herbert Hoover Presidential Library and Museum (LP-HH). Specifically, the OI reviewed (1) the functionality and viability of the RRS used at Archives I and II, (2) the procedures used to issue researcher cards at RW-SB, (3) the procedures used to issue researcher cards at LP-HH, and (4) the potential benefits of implementing a NARA-wide RRS.

BACKGROUND

Office of Inspector General Audit Reports Nos. 08-07 and 10-14

In April 2008 the Office of Inspector General (OIG), Office of Audit (OA) issued OIG Audit Report No. 08-07, *Audit of NARA's Researcher Registration Identification Card Program.* In part the audit found:

"NARA does not utilize a common, integrated technology application for processing, producing and storing researcher card applications at all NARA locations with research rooms," and

"The lack of an automated and uniform processing program, (1) negatively impacts NARA's ability to properly safeguard the records and artifacts entrusted to NARA; and (2) requires researchers to repeat the application process at some NARA facilities."

As a result the audit recommended:

"The Archivist should evaluate the enhanced security and customer service benefits that would accrue to NARA and consider implementing an automated integrated researcher registration system at all NARA facilities with research rooms."

In August 2010, the OA issued OIG Audit Report No. 10-14, *Audit of the Process for Providing and Accounting for Information Provided to Researchers*. In part, the audit found:

"NWC[1] lacks a centralized database to process researcher requests," and

"NARA's ability to effectively identify and/or investigate potential theft of archival documents may be hindered as critical information is not housed in a central location. In the event a researcher is suspected of theft, a centralized database could provide essential information such as (1) photo identification of the suspected researcher; (2) dates and times of the researcher's visits; (3) all NWC locations visited; and (4) all records requested. Additionally, if an individual has stolen from other institutions, a centralized database may help determine if that individual has accessed records at one or more NWC facilities."

As a result, the audit recommended:

"The Assistant Archivist for Records Services – Washington, DC (NW)[2] should implement a centralized database for all of the NW divisions involved in the processing of researchers' requests for records and determine the necessary information that should be included in the database. At a minimum the database should include the elements recorded in the NWCC database."

Although NARA management concurred with the audit recommendations, both remain open and largely unresolved.

Attempts by the OI to Obtain Researcher Access Information

In August 2011, the OI joined the Federal Bureau of Investigation (FBI) in an investigation of Barry Landau and Jason Savedoff. During that investigation, the FBI seized over 10,000 historical items of unknown provenance from Landau's residence. There was immediate evidence Landau and Savedoff had stolen holdings from the Franklin D. Roosevelt Library and

[1] NWC refers to NARA's Access Programs which are now organized under Research Services and broken down into regions and facilities.

[2] The Assistant Archivist for Records Services is now designated as the Executive for Research Services.

Museum. However, in order to determine whether Landau and Savedoff had visited any other Presidential Libraries, the OI had to request data from each library because NARA still did not have a centralized RRS. The OI had no evidence Landau or Savedoff visited any of NARA's regional archives. If they had, the OI would have also had to request a similar data call from all of those facilities.

OBSERVATIONS

1. NARA management has not fully developed a plan to address the recommendations above from OIG Audit Report No. 08-07 and OIG Audit Report No. 10-14. Specifically, NARA still does not have a uniform standard for issuing researcher identification cards or tracking researcher use of NARA facilities.

NARA Efforts to Resolve the Open Audit Recommendations

Over approximately the past year, R has made measurable progress in developing requirements for an automated NARA-wide RRS. However, the audit recommendation from 2008 has largely gone unaddressed for over five years. If NARA management had moved expeditiously to address the recommendation, the OI would have been able to quickly and efficiently determine whether Landau and Savedoff had visited other NARA research rooms. Additionally, had the recommendation been implemented, the RRS at Archives I and II would have already been replaced.

The OI did not assess the current status of the circulation databases mentioned in OIG Audit Report 10-14. However, it is evident from the research room activities the OI did review that NARA management has made no significant progress in implementing a centralized database to process and track researcher requests for documents.

OI Assessment of Researcher Registration Procedures Currently Used at Archives I and II, LP-HH and RW-SB

The OI determined NARA still only has one RRS, which is limited to research rooms at Archives I and II. RW-SB and LP-HH both use paper-based systems and neither maintains an electronic database of researcher card issuance or access. Although all four locations assessed required researchers to provide identification and fill out a form, the identification requirements at RW-SB and LP-HH were not consistent with those used at Archives I and II. In fact, the NARA website states, "Research Card requirements may vary slightly at different facilities."

The RRS used at Archives I and II can capture a photo image of a researcher and record identifying information including name, address and type of identification provided (including any identification numbers i.e. driver's license or passport numbers). The RRS at Archives I and II can also produce a plastic researcher card that includes a photograph. Research room staff at RW-SB and LP-HH reported they also maintain registration paperwork that includes identifying information. However, neither field facility issues researcher cards with photographs or records information from documents provided as proof of identity.

RW-SB staff told the OI the researcher cards issued from that facility are valid at any NARA facility except Archives I and II. However, the LP-HH staff told the OI cards issued from the library are only valid at that location. The OI also observed at both RW-SB and LP-HH that a manual search of either sign-in logs or record pull slips was required to determine if a researcher visited that location.

Suggested Remediation:

The OI suggests NARA management consider:

1. Prioritizing defining, acquiring and implementing an agency-wide RSS. If NARA does not allocate funding and attention to this matter, the 2008 audit recommendation will remain open and unresolved. The continued absence of a centralized NARA RSS may again hinder the OI's ability to quickly and efficiently investigate allegations or discoveries of researcher theft.

2. Planning for a system that could eventually be enhanced and integrated with NARA holdings management systems. An RRS that is capable of tracking researcher requests for documents would directly address the 2010 audit recommendation.

3. Implementing a centralized NARA-wide RRS. The system could be accessed via the NARAnet or Internet from all NARA facilities with research rooms. A centralized RSS would also assist NARA in standardizing policies and procedures for issuing researcher cards throughout all NARA facilities.

4. Executing this project from the Office of the Chief Operating Officer, because this initiative would require collaboration between Research Services (R), the Presidential Libraries (LP) and Information Services (I).

Additionally, a plastic photo researcher credential associated with a specific government issued identification document is more difficult to counterfeit than the paper cards currently issued at RW-SB and LP-HH. If NARA implements such a card agency-wide it may help discourage researchers from providing false information when obtaining a researcher card.

A centralized tracking of researcher access would also allow NARA to conduct data analytics on researcher access. The statistics or trends identified could then assist NARA management in allocating human and fiscal resources to facilities, divisions and projects that involve research services.

2. The RRS used at Archives I and Archives II is at the end of its lifecycle and is not a viable NARA-wide solution.

The OI interviewed research room staff and evaluated the RRS used at Archives I and II. The current RRS has been in use at Archives I and II since 1999, and had been updated and supported by the vendor until approximately five years ago. The OI learned that during the implementation phase of the current system NARA management attempted to gain support for a NARA-wide rollout of the RRS. However, staff at the regional archives and Presidential Libraries strongly opposed agency-wide implementation.

The RRS at Archives I and II is at the end of its life and has limited application and functionality. The OI noted the most reliable part of the current system is the registration portion and not the access data, which could provide an overall picture of how facilities are being used and by which researchers. The RRS and its peripheral components are also largely dependent on the obsolete Windows XP operating system to produce the researcher registration cards.

NARA was unable to provide the OI with documentation that management conducted software lifecycle planning before implementing the current RRS. This planning should have accounted for the eventual replacement of the existing system and provided for the eventual migration of legacy data to a new system. A lack of lifecycle planning suggests NARA took a short-term approach to implementing the RRS, and is now faced with an outdated and unsustainable platform.

NARA research room staff had the following information about the RRS used at Archives I and II:

- the current RRS doesn't have mandatory fields in the database,
- expired researcher cards remain active in the access control system, which would allow a researcher with an expired card to enter research access points,
- data doesn't always properly import from the badge making software to the access control system, and
- researchers aren't given a unique record ID in the system, making it difficult to identify when researchers have had replacement cards made.

NARA research room staff also had the following suggestions:

- require researchers to scan into each research room and scan when they request records
- registration information shouldn't be put into the Holdings Management System, but should be integrated in future deployments,
- any new RRS that should be scalable and deployed nationwide, and
- any new RRS should be a commercial-off-the-shelf (COTS) application that is already in use in other organizations.

The OI did some preliminary research on commercially available software programs that could be implemented across an enterprise network. The OI identified several commercial applications that appeared to be easily implemented across the agency, likely at a significantly lower cost than a custom solution.

Suggested Remediation:

The OI suggests NARA management consider initiating a multidiscipline working group comprised of representatives from R, LP and I. The working group could develop technical requirements for a NARA-wide RSS, and then work with acquisitions to develop a scope of work and identify potential procurement vehicles for a suitable COTS application.

SUMMARY OF RELATED ACTIVITY

Researcher Registration at the National Archives of the United Kingdom

The OI benchmarked researcher registration procedures in place at the National Archives of the United Kingdom (UK Archives). The OI relied upon the first hand experience of an OIG staff member and the procedures detailed on the UK Archives website http://www.nationalarchives.gov.uk/visit/readers-ticket.htm.

The UK Archives requires that researchers obtain a reader's ticket only if they wish to examine original documents. Researchers are not required to have a reader's ticket if they request access to copies of documents, microfilm or microfiche. To obtain a reader's ticket, researchers are required to provide two forms of identification – one form as proof of name and one form as proof of address. The website specifies excepted forms of both.

The reader registration room staff then takes a photograph for the reader's ticket, which is a full head shot without any head or face covering.

Researchers then use their reader's ticket to order original documents using computer terminals in the reading rooms. The OIG staff member familiar with the process explained the UK Archives uses a database to record all requests made by each researcher using a reader's ticket. For example, if a researcher cannot recall what records he has requested in the past, the UK Archives can search his request history.

MANAGEMENT COMMENTS

The OI met with [redacted] Research Services, before and after completing this assessment. Prior to the OI beginning this assessment, [redacted] told the OI he had already begun to address the audit recommendation and assess the viability of the existing database used at Archives I and II. He also indicated he intended to review COTS applications used to issue researcher credentials and track researcher access. Finally, he indicated he intended to look at

networked solutions that could be implemented throughout all of NARA's regional research rooms.

Following the assessment, the OI briefed [redacted] on the observations and suggested remediation reported above. [redacted] also updated the OI on his progress. Specifically, [redacted] reported the Information Technology (IT) Architecture Committee has approved the concept of centralized NARA researcher database and [redacted] will soon begin working an IT contractor to develop system requirements. He also continues to believe there are a number of COTS solutions that will meet the system requirements. He does not support developing a customized system.

CONCLUSION

The RRS currently used at Archives I and II is an aging application with limited potential for expansion and enhancement. The OI suggests NARA management consider replacing it as soon as possible with a NARA-wide solution that will provide for scalability, enhancement and integration with NARA's holding management systems.

Please provide a written response to this Assessment Report within 30 days of the date of issue. As with all OIG products, the OIG will determine what information is publicly posted on the OIG website from this Assessment Report. If you have any suggestions for redactions, please include them with your response. If you have any questions or require additional information, please contact me at 301-837-3000.

cc: David S. Ferriero, Archivist of the United States, N
Debra Wall, Deputy Archivist, ND
Gary Stern, General Counsel, NGC
Bill Mayer, Executive, R
James Gardner, Executive, L
Michael Wash, Executive, I

NATIONAL ARCHIVES

OFFICE *of* INSPECTOR GENERAL

Date : February 6, 2014

Reply to: Acting Inspector General, Office of Inspector General (OIG)

Subject : **Assessment of Critical Incident Law Enforcement Response [redacted] (14-0002-I)**

To : David Ferriero, Archivist of the United States (N)

In September 2013, a single shooter killed 12 people at the Washington Navy Yard. Following that incident, the Archivist of the United States requested that the Acting Inspector General clarify the role of the OIG in an active shooter incident [redacted]. The OIG has no responsibility as a first response law enforcement organization [redacted] so the Office of Investigations (OI) completed an assessment of critical incident law enforcement response [redacted] This was a limited assessment to examine occupant emergency planning, preparedness, and coordination internal [redacted] and external with local law enforcement. This is an informational report meant to convey observations to management, which may then help improve the effectiveness of NARA's emergency response planning [redacted].

Incident response plans and procedures [redacted] are defined in an Occupant Emergency Plan (OEP). Specifically, the OEP contains Emergency Actions Plans (EAPs) for several law enforcement response scenarios including an active shooter event. In summary, the assessment found:

1. the four key personnel identified in the OEP were generally knowledgeable about the OEP; however, three lacked appropriate training to carry out their OEP functions;

2. NARA management has no formal plans or schedule to conduct OEP exercises;

3. the Chief of Security [redacted] has not routinely coordinated with local law enforcement, and;

4. there are no Security Management Branch (BX) representatives [redacted] on weekends and holidays.

BACKGROUND

[redacted] *Occupant Emergency Plan*

On July 5, 2012, the BX conducted a security assessment [redacted]. Based on Department of Homeland Security (DHS), Interagency Security Committee (ISC) standards, the BX classified [redacted] as a Security Level [redacted] facility. The classification was based in part on the historical significance of NARA's holdings and because the building is [redacted].

In October 2013, the Chief of Security prepared and NARA management approved an OEP [redacted] *Occupant Emergency Programs: An Interagency Security Committee Guide, March 2013* (ISC Guide), defines an OEP as "a written set of procedures to protect life and property in a facility under specific emergency conditions." The [redacted] OEP defines the roles and responsibilities of key NARA personnel, and establishes EAPs for specific emergencies. The Facilities Management Branch (BF) has primary responsibility for the OEP.

Facility Security Committee

[redacted] has a formal Facility Security Committee (FSC) that meets approximately every two months to discuss the OEP, EAPs, and other internal operating procedures that impact security [redacted] The Chief of Security prepared and the FSC approved the recently updated OEP and associated EAPs [redacted].

SCOPE

The OI generally assessed emergency planning for critical incident scenarios identified in [redacted] OEP that require a law enforcement response. Specifically, the OI reviewed (1) the roles and responsibilities of NARA employees responsible for executing the OEP, (2) whether NARA conducts training and exercises to test OEP planning and preparedness, and (3) whether NARA management coordinates regularly with local law enforcement.

OBSERVATIONS

1. Key personnel are not familiar with the OEP and have not been properly trained.

Designated Official and Alternate Designated Official

The OEP identifies the Designated Official as a senior representative responsible for (1) executing the OEP [redacted], (2) ensuring staff is trained to respond in accordance with the OEP, and (3) ensuring drills and exercises are conducted at least annually. The Archivist of the United States has overall command authority [redacted] However, the Archivist selected the Director of [redacted] as the Designated Official to act for him during emergencies. The Archivist selected the Director of [redacted] as the alternate Designated Official.

Both the Designated Official and the alternate Designated Official (Directors) stated the Chief of Security gave them the OEP to review in September 2013. The Directors and the Chief of Security also visited the security control center to familiarize the Directors with emergency incident procedures. Although the Directors stated they were generally familiar with the OEP and with security control operations, neither were aware the OEP makes them responsible for evacuation and emergency operations during a critical incident involving local law enforcement. Additionally, neither Director has received any formal training in incident command or response. Finally, the Directors did not know the OEP Occupant Emergency Coordinator is [redacted] Building Manager, not the Chief of Security.

Occupant Emergency Coordinator

The OEP states the Occupant Emergency Coordinator is responsible for (1) identifying personnel required to carry out the OEP, (2) establishing working relationships with other Federal and local agencies having emergency responsibilities, (3) scheduling and coordinating training and drills to ensure the safe evacuation/relocation of personnel in the event of an emergency, (4) coordinating Memorandums of Understanding (if any) with local emergency personnel and (5) coordinating the activities of local emergency personnel, other government agencies, and other support personnel during an emergency.

The Building Manager was unaware they had been assigned as the Occupant Emergency Coordinator, and did not know where their position fell on the OEP organizational chart. The Building Manager recalled reviewing the OEP, but they were unaware that the BF was responsible for the plan. Rather, they thought the Chief of Security and the BX were responsible for managing the plan. The Building Manager explained that because the Chief of Security created the OEP, they assumed the BX was the responsible office.

The Building Manager noted that prior to 9/11 most government buildings had OEPs primarily for natural disasters, so the facilities department was typically responsible for drafting, implementing, and testing the plan. The Building Manager further noted that after 9/11 most OEPs were changed to reflect terrorist threats and the OEP became more of a security function. The Building Manager believed the Chief of Security was responsible for law enforcement liaison.

Security Coordinator

The Security Coordinator is the Chief of Security [redacted]. The Chief of Security prepared the OEP and represents NARA at ISC meetings. The OEP indicates the Chief of Security is responsible for (1) providing support and guidance on security related matters to the Designated Official, (2) developing, coordinating, and maintaining the Building Security Plan and security response protocols, (3) maintaining personnel and site security during emergency situations, and (4) assisting in the collection of information for local law enforcement authorities.

The Chief of Security confirmed the Building Manager is the primary point of contact in the event of a building evacuation. However, the Chief of Security stated if a critical incident requires a law enforcement response, they are the primary point of contact instead of the Building Manager. The Chief of Security explained the Building Manager is not trained in physical security, so the Building Manager is only qualified to handle critical incidents involving natural disasters or fire. Although the Chief of Security was clear about this defined split in responsibilities, they could not cite where the OEP defines this change in command structure.

Suggested Remediation:

The OI suggests senior NARA management consider revising the OEP to reflect the personnel responsible for decision-making and operations during critical incidents involving a law enforcement response. Additionally, the OI suggests NARA management consider formally assigning BX responsibility for the OEP. Finally, the OI suggests the Directors immediately develop a training curriculum for all key OEP personnel.

2. The Directors do not have a plan or schedule to conduct exercises to test NARA and local law enforcement response in accordance with the OEP.

The OEP requires the Directors to schedule and conduct Security Level [redacted] training and exercises to test critical incident law enforcement response. However, the Directors have neither conducted nor scheduled any training or drills [redacted]. Additionally, the Directors were not aware of their responsibility to conduct emergency exercises and instead thought the Chief of Security was responsible.

The Chief of Security stated BX has not conducted any critical incident response drills [redacted] because [redacted]. The Chief of Security also has no future plans to conduct any critical incident response drills. The Chief of Security further explained he does not see a need to perform drills for incidents requiring a law enforcement response because the [redacted] Police Departmen[redacted] responds quickly to all calls [redacted].

Suggested Remediation:

The OI suggests the Directors consider establishing a plan to conduct a critical incident law enforcement response exercise [redacted] within the next calendar year. NARA management could conduct the exercise after hours or use tabletop[1] scenarios. The Directors should ensure the MPD participates in the planning and execution of all scheduled drills.

[1] According the ISC Guide tabletop exercises are discussions-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles and responses during an emergency. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, thus initiating a discussion among the participants of roles, responsibilities, coordination, and decision-making.

3. The Chief of Security does not regularly coordinate with local law enforcement.

The OEP identifies [redacted] as the local law enforcement agency responsible for responding to [redacted] However, the OEP makes no specific reference to the [redacted], the specialized [redacted] responsible for the majority of incidents described in the OEP. The Chief of Security refers information and intelligence to [redacted], but the material referred to [redacted] often relates to general, nonspecific threats received at [redacted]

A sergeant with [redacted] confirmed [redacted] has predominant jurisdiction at [redacted] and that [redacted] would be dispatched to respond to a critical incident. The sergeant was aware [redacted] is not covered by [redacted], but stated [redacted] has not visited [redacted] since 2009. Additionally, [redacted] has no functional knowledge of the OEP, [redacted] floor plans, and the number of employees and visitors in the building.

The sergeant would like to assess the building and expressed an interest in using parts of the building to conduct training and drills for his specialized units. The sergeant explained having drills and training in the building increases the effectiveness of first responders. Finally, the sergeant indicated it would be beneficial for [redacted] to understand their responsibility and jurisdiction, because [redacted] is not a [redacted] building.

Suggested Remediation:

The OI suggests the Directors require the Chief of Security to arrange for representatives from [redacted] to tour [redacted] and meet with key OEP and security personnel. Additionally, the OI recommends NARA management consider establishing regular meetings with [redacted] to share OEP related information and intelligence. The Chief of Security should also consider documenting all formal coordination with local law enforcement, other security directors, and other Federal agencies.

4. There is no BX presence at [redacted] on weekends and holidays when the building is open to the public.

[redacted] are open to the public [redacted] and the research rooms operate Monday through Saturday. NARA personnel serve and supervise researchers at all times while the research rooms are open to the public. However, during weekends and Federal holidays there are no BX personnel [redacted]. Security staff on those days is limited to contract security guards.

In the event of a critical incident at [redacted] over the weekend or on a holiday, the OEP would be initiated by a contract engineer on duty and/or a contract security supervisor. The Chief of Security stated appropriate contract employees would assume command and control until local law enforcement arrive. The Chief of Security also stated contract personnel have been trained on how to respond to a critical incident at [redacted] in the absence of BX personnel.

In comparison, the [redacted], the [redacted], and the [redacted] all have Federal security or police personnel at their facilities [redacted] 24 hours a day, 365 days a year.

Suggested Remediation:

The OI suggests NARA management consider staffing [redacted] with a security specialist during all hours the facility is open to the public. Additionally, the OI suggests the Chief of Security formally explore the cost and security benefits of using Federal employees (General Series – 0085) instead of contract security guards [redacted].

SUMMARY OF RELATED ACTIVITY

[redacted]

MANAGEMENT COMMENTS

The OI discussed the results of this assessment with the Executive for Business Support Services and the agency Security Officer. Both generally concurred with the observations and suggested remediation. However, the Security Officer asked that the report reflect that additional full-time equivalents or funding may be necessary to implement the remediation suggested under Observation 4.

Please provide a written response to this Assessment Report within 30 days of the date of issue. If you have any questions or require additional information, please contact me or Matthew Elliott, my Assistant Inspector General for Investigations, at 301-837-2941.

James Springs
Acting Inspector General

cc: Jay Bosanko, Chief Operating Officer, C
Charles Piercy, Executive, B
Kevin McCoy, Security Officer, BX
Debra Wall, Deputy Archivist, ND

NATIONAL ARCHIVES

OFFICE *of*
INSPECTOR GENERAL

Date : April 24, 2014

Reply to: Acting Inspector General, Office of Inspector General (OIG)

Subject : **Assessment of Critical Incident Law Enforcement Response [redacted] (14-0003-I)**

To : David Ferriero, Archivist of the United States (N)

In September 2013, a single shooter killed 12 people at the Washington Navy Yard. Following that incident, the Archivist of the United States requested that the Acting Inspector General clarify the role of the OIG in an active shooter incident [redacted]. The OIG has no responsibility as a first response law enforcement organization [redacted], so the Office of Investigations (OI) completed an assessment of critical incident law enforcement response [redacted]. This was a limited assessment to examine occupant emergency planning, preparedness, and coordination internal [redacted], and external with local law enforcement. This is an informational report meant to convey observations to management, which may then help improve the effectiveness of NARA's emergency response planning [redacted].

Incident response plans and procedures for [redacted] are defined in an Occupant Emergency Plan (OEP). Specifically, the OEP contains Emergency Actions Plans (EAPs) for several law enforcement response scenarios including an active shooter event. In summary, the assessment found:

1. the three key personnel identified in the OEP were generally knowledgeable about the OEP; however, all three lacked specific OEP training to carry out their OEP functions;

2. the Security Coordinator was unsure if [redacted] or another local law enforcement agency would respond to [redacted] during a critical incident, and;

3. the Designated Official does not have a plan or schedule to conduct exercises to test NARA and local law enforcement response in accordance with the OEP, and;

4. there are no Security Management Branch (BX) representatives at [redacted] when the building is open to researchers.

BACKGROUND

[redacted] *Occupant Emergency Plan*

In August 2011, the BX conducted a security assessment of [redacted] Based on Department of Homeland Security (DHS), Interagency Security Committee (ISC) standards, the BX classified [redacted] as a Security Level [redacted] facility. The classification was based in part on the historical significance of NARA's holdings and the number of employees, students and contractors assigned to the facility.

In January 2013, the Facility & Property Management Division (BF) approved an OEP for [redacted] *Occupant Emergency Programs: An Interagency Security Committee Guide, March 2013* (ISC Guide), defines an OEP as "a written set of procedures to protect life and property in a facility under specific emergency conditions." The [redacted] OEP defines the roles and responsibilities of key NARA personnel, and establishes EAPs for specific emergencies. The BF has primary responsibility for the OEP.

Unlike [redacted] has no formal Facility Security Committee that meets to discuss the OEP, EAPs, and other internal operating procedures that impact security.

SCOPE

The OI generally assessed emergency planning for critical incident scenarios identified in the [redacted] OEP that require a law enforcement response. Specifically, the OI reviewed (1) the roles and responsibilities of NARA employees responsible for executing the OEP, (2) whether NARA conducts training and exercises to test OEP planning and preparedness, and (3) whether NARA management coordinates regularly with local law enforcement.

OBSERVATIONS

1. Key personnel are familiar with the OEP, but they have not been properly trained.

Designated Official and Alternate Designated Official

The OEP identifies the Designated Official as a senior representative responsible for (1) executing the OEP for [redacted], (2) ensuring staff is trained to respond in accordance with the OEP, and (3) ensuring drills and exercises are conducted at least annually. The Archivist of the United States has overall command authority [redacted]. However, the Archivist selected the [redacted] as the Designated Official to act for him during emergencies.

The Designated Official stated the Team Leader gave him the OEP to review in January 2013. The Designated Official was generally familiar with the OEP and with security control operations. The Designated Official was also aware the OEP makes him responsible for evacuation and emergency operations during a critical incident involving local law enforcement. The Designated Official has not been trained in incident command or response. Rather, the Designated Official stated he relied on experience from working at another Federal agency.

Occupant Emergency Coordinator

The [redacted] Occupant Emergency Coordinator is the [redacted] (hereafter, the Director). The OEP states the Occupant Emergency Coordinator is responsible for (1) identifying personnel required to carry out the OEP, (2) establishing working relationships with other Federal and local agencies having emergency responsibilities, (3) scheduling and coordinating training and drills to ensure the safe evacuation/relocation of personnel in the event of an emergency, (4) coordinating Memorandums of Understanding (if any) with local emergency personnel and (5) coordinating the activities of local emergency personnel, other government agencies, and other support personnel during an emergency.

The Director was knowledgeable about the OEP and knew where his position fell on the OEP organizational chart. The Director stated prior to 9/11 most government buildings had OEPs primarily for natural disasters, so the facilities department was typically responsible for drafting, implementing, and testing the plan. However, the Director stated that after 9/11 most OEPs were changed to reflect terrorist threats and the OEP became more of a security function. The Director believed the Team Leader should be responsible for law enforcement liaison. The Director stated he was not formally trained for his OEP responsibilities, but instead relies on his past [redacted] experience.

Security Coordinator

The Security Coordinator is the Physical Security Team Leader (hereafter, the Team Leader) at [redacted] The OEP indicates the Security Coordinator is responsible for (1) providing support and guidance on security related matters to the Designated Official, (2) developing, coordinating, and maintaining the Emergency Action Plan and security response protocols, (3) maintaining personnel and site security during emergency situations, and (4) assisting in the collection of information for local law enforcement authorities.

The Team Leader confirmed the Director is the primary point of contact in the event of a building evacuation. However, the Team Leader stated if a critical incident requires a law enforcement response, they would be the primary point of contact instead of the Director. The Team Leader also said it would be more appropriate to assign them as the Occupant Emergency Coordinator, but BX would need more personnel to handle the additional responsibilities.

Suggested Remediation:

The OI suggests senior NARA management consider revising the OEP to reflect the personnel responsible for decision-making and operations during critical incidents involving a law enforcement response. Additionally, the OI suggests NARA management consider formally assigning BX responsibility for the OEP. Finally, the OI suggests the Designated Official immediately develop a training curriculum for all key OEP personnel.

2. The Security Coordinator was unsure if [redacted] or another local law enforcement agency would respond to [redacted] during a critical incident.

The Team Leader stated BX has not conducted any critical incident response drills [redacted], and stated better coordination with local police and fire departments would be beneficial. The Team Leader again stated BX could do more with additional personnel.

The OEP identifies the [redacted] as the local law enforcement agency responsible for responding to [redacted] However, after BX and BF finalized the current OEP, NARA eliminated the reimbursable agreement between NARA and [redacted] because of budget cuts. The Team Leader stated [redacted] would be the most likely first responder in the event of a critical incident. However, they have never coordinated with [redacted] and stated [redacted] might respond if [redacted] has a mutual assistance agreement with [redacted]. The NARA Security Officer later clarified that because [redacted] lies within [redacted] is the first-response law enforcement agency responsible for the facility.

Suggested Remediation:

The OI suggests the Designated Official require the Team Leader to update the OEP to identify [redacted] as the local law enforcement agency responsible for [redacted].

The Team Leader should also consider providing [redacted] with a tour of [redacted], and arranging a meeting between [redacted] and key OEP and security personnel. Additionally, the OI recommends NARA management consider establishing regular meetings with [redacted] to share OEP related information and intelligence.

3. The Designated Official does not have a plan or schedule to conduct exercises to test NARA and local law enforcement response in accordance with the OEP.

The OEP requires the Designated Official to schedule and conduct Security Level [redacted] training and exercises to test critical incident law enforcement response. However, the Designated Official has neither conducted nor scheduled any training or drills (related to law enforcement response) at [redacted]

Suggested Remediation:

The OI suggests the Designated Official establish a plan to conduct a critical incident law enforcement response exercise at [redacted] within the next calendar year. NARA management could conduct the exercise after hours or use tabletop[1] scenarios. The Designated Official should ensure [redacted] participates in the planning and execution of all scheduled drills.

4. There is no BX presence at [redacted] when the building is open to the public.

[redacted] is open to researchers [redacted]. However, there are no BX personnel on duty on [redacted]. In the event of a critical incident at [redacted] a contract engineer on duty and/or a contract security supervisor would initiate the OEP. The Team Leader stated appropriate contract employees would assume command and control until local law enforcement arrive. The Team Leader also stated contract personnel have been trained on initiating the OEP during a critical incident at [redacted] in the absence of BX personnel.

Suggested Remediation:

The OI suggests NARA management consider staffing [redacted] a security specialist during all hours the facility is open to the public. Additionally, the OI suggests the Team Leader formally explore the cost and security benefits of using Federal employees (General Series – 0085) instead of contract security guards at [redacted]

MANAGEMENT COMMENTS

The OI met with NARA management to discuss the results of this assessment and seek clarity to unresolved requests for information. NARA management provided the OI with all necessary information and the OI distributed a draft report for review and comment. Management requested the OI clarify sections of the report related to Observations 2 and 3. As a result, the OI clarified that the Team Leader stated [redacted] might respond

[1] According to the ISC Guide, tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles and responses during an emergency. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, thus initiating a discussion among the participants of roles, responsibilities, coordination, and decision-making.

[redacted]) if [redacted] has a mutual assistance agreement with [redacted].
Additionally, the OI copied the more specific language from Observation 3 to the summary bullets on page 1.

Please provide a written response to this Assessment Report within 30 days of the date of issue. If you have any questions or require additional information, please contact me or Matthew Elliott, my Assistant Inspector General for Investigations, at 301-837-2941.

James Springs
Acting Inspector General

cc: Jay Bosanko, Chief Operating Officer, C
Charles Piercy, Executive, B
Kevin McCoy, Security Officer, BX
Debra Wall, Deputy Archivist, ND

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

REPORT OF INVESTIGATIONS

Case Number: 09-002-I

WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

REPORT OF INVESTIGATION

Title (Name and address):	Type of Investigation:	Type of Report:
[redacted]	Criminal/Administrative	☒ Final ☐ Supplemental

Social Security Number: N/A	☐ Employee ☒ Non-employee ☐ Former Employee	
Date of Birth: N/A	Date Entered on Duty: N/A	Position and Grade: N/A
Post of Duty: N/A	Organization and Office: N/A	
Period of Investigation: October 2008 – November 2010		

BASIS FOR INVESTIGATION

On October 28, 2008, [redacted], Contracting Officer's Representative (COR), National Archives and Records Administration (NARA), told NARA's Office of Inspector General (OIG), that [redacted] supplied equipment under NARA contract number [redacted] that was possibly grey market material. In addition, the material might have been manufactured in foreign countries to include China and Hungary.

ALLEGED VIOLATIONS

18 U.S.C. § 371 Conspiracy
18 U.S.C. § 1343 Wire Fraud
18 U.S.C. § 2 Aiding and Abetting

RESULTS OF INVESTIGATION

The OIG substantiated that [redacted] provided counterfeit and grey market Cisco equipment to NARA, purchased from an unauthorized distributor, [redacted]. The United

Distribution	No.	Case Number:	Signature of Special Age[illegible]aking Report:
Office of Inspector General	1	09-002-I	
National Archives and Records Administration, General Counsel	2	Signature of Person Examining Report:	
Assistant U.S. Attorney			
Other *(Specify)*:		Title: Assistant Inspector General for Investigations	Office*(City)*: College Park, MD
		Division Office: Headquarters	Date of Report: 4/20/11

States Attorney's Office for the Southern District of Maryland declined prosecution [redacted]

(B)(5)
Per EOUSA

[redacted]

The OIG prevented the undue payment of $1,149,100 to [redacted] for counterfeit and grey market products.

INVESTIGATIVE SUMMARY

EXHIBIT

Background

Cisco products and services are sold through a network of Cisco Authorized Channel Partners. Cisco's Authorized Channel Partners are required to resell Cisco Products and Services in a given territory, as set forth in contractual agreements with Cisco. The base level partner is a Select Partner, and the top-level partner is a Gold Partner. Cisco products are sold with end user warranties. These warranties are personal to the first end user and, unless expressly authorized by Cisco, the warranty may not be transferred to any new purchaser of the Cisco products. Thus, any product that is not purchased through the legitimate Cisco Authorized Channel does not come with a valid warranty. Cisco's service and support model allows for customers to purchase additional service coverage on Cisco's networking equipment in the event the customer needs assistance in troubleshooting technical problems or replacement of faulty parts. These service contracts are called SMARTnet contracts. Customers may choose from a variety of support and contract offerings depending on the nature of service they wish to receive. SMARTnet contracts are available to the first end user of a product, and Cisco requires that a second end user may obtain a SMARTnet contract only after paying to have the product re-inspected and paying for licenses for the software that is installed on the product.

On [redacted], 2008, via the Federal Business Opportunities (FedBizOpps) website, NARA publicly announced NARA solicitation [redacted] issued as a request for quotation (RFQ). There were 18 line items listed. One of the line items 1, 2

was for 14 SMARTnet service contracts for 14 equipment pieces, [redacted]. During the contractual Questions and Answers session, an unidentified vendor asked if NARA would accept Cisco equipment that was not sourced from a certified Cisco partner. NARA responded with an Amendment of Solicitation/ Modification of Contract, Standard Form 30, which clarified ". . . NARA requires that all Cisco products be purchased from 'Authorized/Certified Vendor's only.' Any and all vendors submitting quotes shall provide proof of authorization from Cisco." [redacted] responded to the NARA FedBizOpps announcement with an undated quotation in which [redacted] indicated they would supply "new" Cisco equipment. [redacted] stated they were an authorized Cisco Select Partner. [redacted] submitted a quote for $1,149,100 and offered the following: 1) Assembly and configuration of the chassis at no additional cost should the government wish to take advantage of this option; and 2) a one year performance replacement level warranty **[Agent Note:** This is not a Cisco Warranty.]

On [redacted], 2008, NARA awarded [redacted] the contract. On [redacted] 2008, Cisco notified [redacted] that they would be removed from the Cisco Partner program. On [redacted], 2008, NARA received equipment from [redacted] via [redacted]. [redacted] NARA's COR, notified the OIG that the labels on the equipment indicated the equipment originated from China, Hong Kong, and Hungary; and Cisco informed the equipment was grey market. [redacted] explained that grey market meant the equipment originated outside of the Cisco approved distribution channels. The serial numbers and other forensic data were provided to Cisco for further assessment. Cisco told the OIG that 41 pieces of equipment were counterfeit, in that the equipment was Cisco brand equipment but the original labels had been removed and replaced with false labels. The 41 pieces consisted of [redacted]. The remainder of the equipment was identified as grey market, as it was sold outside of authorized Cisco distribution channels. Counterfeit equipment is ineligible for SMARTnet service contracts. To support the grey market equipment with SMARTnet service contracts, Cisco would require NARA to pay an additional fee to reexamine and license the equipment.

Interviews/Investigative Actions

PRIOR TO AWARD

On September 12, 2008, in response to RFQ clarification questions, [redacted] Systems Development Division (NHV), NARA, emailed the NARA Acquisition Analyst, [redacted] and advised that the Cisco equipment purchased by NARA must be new and must have Cisco authorized service. **[Agent Note:** The word "new" was omitted

from the NARA RFQ; however, [redacted] bid specified that all parts would be new.]

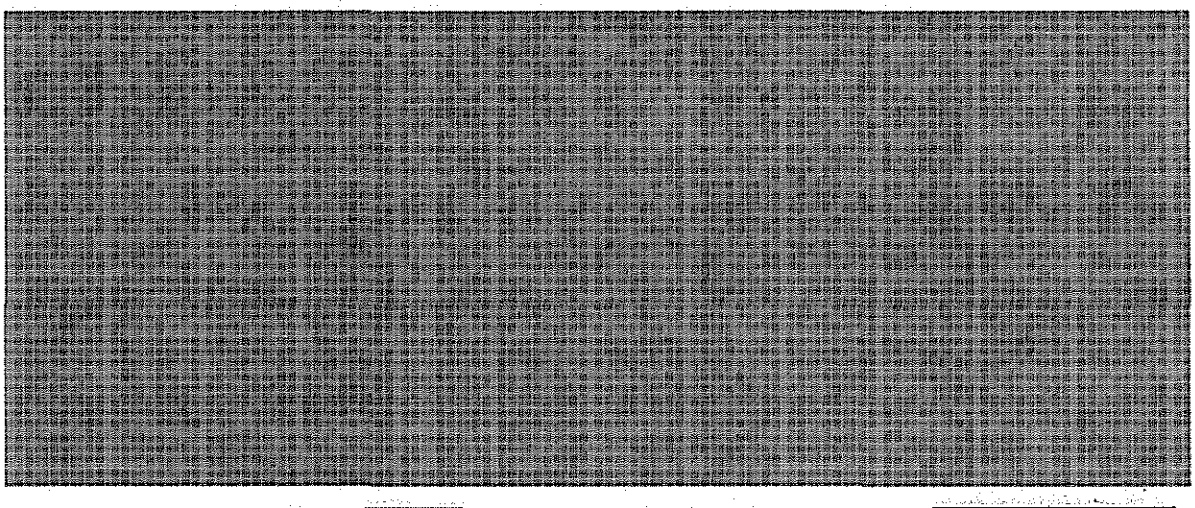
POST AWARD

On September 26, 2008, [redacted], Brand Protection Group, Cisco, emailed [redacted], and asked for the source of the NARA equipment. [redacted] advised that [redacted] discounting was higher than what is given to large Gold Partners and a high discount on this deal would require a deviation from the Cisco Sales Team. In this case no deviation was given. [redacted] told [redacted] that per [redacted] contract with Cisco as an authorized reseller, [redacted] is only able to purchase Cisco services and products from an authorized distributor [redacted] and to resell such Cisco services and products directly to end users. [redacted] advised [redacted] that resold Cisco products that have been sourced outside of Cisco's authorized channels do not come with a valid software license or hardware warranty. Cisco reserves the right to refuse support on any secondary market sourced product, even if presented with a valid SMARTnet contract. Proof must be presented that the product has undergone an inspection by Cisco, and appropriate software licenses are procured. [redacted] told [redacted] that [redacted] suppliers were [redacted]. [**Agent Note:** At the time of the NARA RFQ, [redacted] were authorized Cisco distributors. [redacted] actual suppliers were [redacted] At the time of this award, [redacted] was not an authorized Cisco distributor or a Channel Partner. [redacted] coordinated with [redacted] to provide [redacted] the Cisco equipment. At the time of this award, [redacted] was not an authorized Cisco distributor or a channel partner.] 4

On September 29, 2008 and September 30, 2008, [redacted], [redacted], [redacted] 5, 6

(B)(5)
Per EOUSA

Case Title:	Case Number:
[redacted]	09-002-I



(B)(5)

Per EOUSA

On September 30, 2008, [redacted] emailed NARA CO representative [redacted] stating the equipment they would supply NARA would be ". . . new, genuine Cisco, and it comes with a one-year warranty. A Cisco-certified engineer will be on-hand for a day to receive and test the equipment when it arrives at NARA." 7

On October 1, 2008, [redacted] emailed [redacted] to advise that [redacted] was contacted by Cisco Account Manager [redacted] who indicated that the equipment [redacted] quoted was "sourced outside the channel and not from an authorized distributor." [redacted] further indicated the equipment would not be supported. [redacted] told they would honor their commitments and meet [redacted] expectations. 8

On October 1, 2008, [redacted], Cisco [redacted], emailed [redacted] to advise that [redacted] failure to disclose information about the Cisco authorized distributor they plan to procure NARA products from severely jeopardized the status of [redacted] reseller agreement with Cisco. Additionally, Cisco Brand Protection reserves the right to terminate the Channel Partner agreement between [redacted] and Cisco. 9

On October 2, 2008, [redacted], a Cisco representative, emailed [redacted] to thank [redacted] for discussing the risk NARA may have with the award to [redacted]. [redacted] advised Cisco would be seeking action against [redacted] due to [redacted] unwillingness to fulfill the NARA purchase through the Cisco authorized channel. [redacted] suggested there was a risk that [redacted] supplied grey market product. 10

On or about October 6, 2008, [redacted] and [redacted] met with [redacted] and [redacted] At no time did [redacted] tell [redacted] tha[redacted] was a reseller or state that [redacted] was a supplier of grey market Cisco products. [redacted] assured [redacted] that 11

NARA would receive the equipment as requested. [redacted] questioned whether the equipment would be used or second hand. [redacted] denied the equipment would be grey market/used and would be packaged to show that it was new. [redacted] responded that [redacted] and [redacted] would get the equipment supported by Cisco certified technicians. [redacted] told [redacted] that Cisco representatives wanted [redacted] to believe they would not support the equipment but they would, in fact, support it. [redacted] checked the Cisco website and it indicated [redacted] was a Cisco partner. Despite Cisco telling [redacted] they would not support the equipment, [redacted] believed [redacted] had the ability to make Cisco support the equipment. During this time, [redacted] called [redacted] and told [redacted] that Cisco would not suppor[redacted] and Cisco had removed [redacted] from their partner list. [redacted] went onto Cisco's website and could no longer confirm [redacted] was listed as a Cisco partner. [redacted] became concerned as Cisco was the manufacturer and they told [redacted] they were not going to support the product. In addition, Cisco told [redacted] the equipment may be counterfeit. [redacted] took no action.

On October 28, 2008, [redacted] told NARA's OIG that [redacted] supplied equipment under NARA contract number [redacted] that was possibly grey market material. In addition, the material might have been manufactured in foreign countries to include China and Hungary. 12

On October 30, 2008, the OIG contacted Cisco to discuss the Cisco equipment NARA purchased. [redacted] said due to concerns about the origin of the Cisco equipment, Cisco questioned [redacted] about where they sourced the equipment. [redacted] was not clear with Cisco about their distributor and did not confirm they would use Cisco certified distributors to fulfill the equipment order. Cisco checked a partial list of the serial numbers associated with the NARA contract order and determined that the equipment they researched was grey market. [redacted] advised grey market equipment is equipment purchased outside of permitted Cisco channels. [redacted] told the OIG that grey market merchandise can be new, used or counterfeit. [redacted] revealed the following concerning 11 serial numbers [redacted] researched from the equipmen[redacted] provided to NARA: 1) Two were pieces of equipment originally sold in Atlanta, GA; 2) six were sent to Germany; and 3) three went to Bangladesh[redacted] did not purchase this equipment from Cisco or a Cisco certified distributor, thus, the equipment was grey market equipment. 13

14

[redacted]

15

On December 1, 2008, the OIG interviewed [redacted] and [redacted] said that after he saw NARA's RFQ on FedBizOpps, [redacted] submitted an RFQ to several companies to include [redacted] to buy the equipment to support the NARA contract. [redacted] bid the lowest price and [redacted] agreed to buy the equipment from [redacted]. [redacted] said that [redacted] did not know about [redacted] supplying the equipment until [redacted] scheduled a meeting with [redacted] and [redacted] was contacted by [redacted] sales representative [redacted] at which time [redacted] advised [redacted] that [redacted] would attend the meeting with [redacted] and NARA.

16

Cisco, via their legal counsel, provided the OIG a redacted copy of their findings pertaining to the equipment provided to NARA by [redacted] and [redacted] for inclusion in this report. Their report indicated that 40 of the [redacted] and 1 of the [redacted] [misidentified in the conclusion of the repor[redacted] were counterfeit. It was determined that all of the [redacted] were stolen prior to official sale by Cisco. All of the

17

[redacted] were labeled with false serial numbers, some of which were duplicated in that they were assigned to other Cisco products and the Media Access Control (MAC) addresses were assigned to other Cisco products or other manufacturers. The [redacted] appeared to have been stolen from a contract manufacturer, but in addition it was defective and should have been scrapped. The [redacted] was labeled with a false serial number and a MAC address assigned to another [redacted].

[redacted] told the OIG that [redacted] of [redacted], brought the NARA deal to [redacted]. [redacted] was partnering with [redacted]. Companies like [redacted] seek out small businesses because they know that the federal government likes to contract and support small business such as [redacted]. [redacted] knows that the small business will get the contract but will have difficulty funding the deal. [redacted] will contact these companies and offer to support them in their contracts with the federal government. [redacted] would have never been able to support the NARA contract without companies like [redacted] and [redacted] and [redacted] employee [redacted] worked with [redacted] on the NARA contract. [redacted] understood that the equipment for NARA was for "brand new" equipment. Brand new meaning it was not used and had not been "put in service." [redacted] said that [redacted] has no affiliation with Cisco, is not a Cisco partner, and does not have any official access to the Cisco database. [redacted] said that [redacted] uses other companies to assist [redacted] with SMARTnet coverage. [redacted] said that "a lot of relationships we have were people doing things they were not supposed to do, but it happens every day in our industry." [redacted] cited the example of using [redacted], to research serial numbers in Cisco's database. As long as [redacted] could acquire information on serial numbers and end user contact information, they could help [redacted] get coverage. [redacted] believed that [redacted] had a relationship with Cisco that allowed them to acquire coverage. Another company that assisted [redacted] in SMARTnet coverage for the NARA equipment was [redacted]

18

[redacted], Cisco Investigator, told the OIG that [redacted] purchased SMARTnet for [redacted] and registered NARA as the "end user" on [redacted] 2008. [redacted] should not have been able to acquire a SMARTnet contract for these [redacted] as NARA was not the original end user. The original end user, [redacted] located in Sweden, purchased at least 2 of the 13 [redacted] in [redacted] 2008. [redacted] explained at the time of [redacted] purchase, these [redacted] would come with original purchase warranties but, the warranty was voided once [redacted] sold the [redacted] to another company, as warranties do not transfer.

19

[redacted] provided counterfeit and grey market Cisco equipment to NARA, purchased from an unauthorized distributor, [redacted]. The United States Attorney's Office for the

Southern District of Maryland declined prosecution [redacted]

(B)(5)

Per EOUSA

[redacted] The OIG prevented the undue payment of $1,149,100 to Biztech for counterfeit and grey market products.

Exhibit Number	Description
1	NARA Request for Quote with Attached Solicitation Modification, September 10, 2008
2	[redacted] Quotation For Cisco Equipment, undated
3	Email from [redacted], Subject: Fwd: RE: [redacted], dated September 12, 2008
4	Email from [redacted], Subject: RE: Cisco Systems Follow-up for National Archives, dated September 26, 2008
5	Email from [redacted], Subject: Necessary Information- Read these documents!!!, dated September 29, 2008
6	Email from [redacted] Subject: RE: Cisco equipment supply confirmation, dated September 30, 2008
7	Email from [redacted], Subject: [redacted] Award, dated [redacted], 2008
8	Email from [redacted], Subject : FW: [redacted], dated [redacted], 2008
9	Email from [redacted], Subject: Cisco NARA Deal, dated October 1, 2008
10	Email from [redacted], Subject: Notification of Risk and Cisco Systems Follow-up for Fed Biz Ops Solicitation [redacted], dated [redacted], 2008
11	Memorandum of Interview, [redacted], dated June 18, 2009
12	Memorandum of Activity, [redacted] Employee Notifies About Equipment, dated October 28, 2008
13	Memorandum of Interview, Teleconference with Cisco Representatives, dated October 30, 2008
14	[redacted]
15	[redacted]
16	Memorandum of Interview, [redacted] and [redacted], [redacted], dated December 1, 2008
17	Memorandum of Activity, Redacted Cisco Report Approved by Cisco, dated December 23, 2010
18	Memorandum of Interview, [redacted], dated June 29, 2010
19	Memorandum of Interview, Teleconference with [redacted], Investigator, Criminal/Service Fraud, Cisco, and [redacted], Trial Attorney, Public Integrity Section (PIS), Department of Justice (DOJ) and Cisco, dated July 22, 2010

Case Number:	Case Title:
09-002-I	[redacted]

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	Type of Report:
10-0011-I	Stolen Valor Veteran Record Fraud	☐ Interim ☒ Final ☐ Supplemental
Type of Investigation: ☒ Criminal ☐ Civil ☐ Administrative ☐ Information		**Period of Investigation:** December 2009 - February 2011

SUBJECT(S) OF INVESTIGATION

Primary Subject:

[redacted]

BASIS FOR INVESTIGATION

On December 7, 2009, [redacted], Reference Core 5, National Personnel Records Center Military Records (NPRC-MR), National Archives and Records Administration (NARA), St. Louis, MO, forwarded to the Office of Inspector General, Office of Investigations (OI), allegations [redacted], a member of the Military Order of the Purple Heart (MOPH), [redacted], altered/falsified NARA documents.

ALLEGED VIOLATIONS

18 U.S.C. § 704 (a)(b)(d), False Claims Relating to Military Medals and Decorations
18 U.S.C. § 498, Military or Naval Discharge Certificates
18 U.S.C. § 506, Seals of Departments or Agencies
18 U.S.C. § 912 False Impersonation, Officer or employee of the United States
[redacted]
18 U.S.C. § 1343, Wire Fraud
[redacted]
18 U.S.C. § 1001, False Statements

Prepared by:	Approved by: AIGI Matthew Elliott	Date of Report:
[redacted]	Signature: [signature]	March 13, 2012

REPORT OF INVESTIGATION (Continued)

RESULTS OF INVESTIGATION

Preliminary OI Investigation

An OI review of [redacted] official military records revealed [redacted] lied about [redacted] military service and age to MOPH and the U.S. Department of Veterans Affairs (VA). Additionally, it was discovered that [redacted] received an Article 15 for changing [redacted] date of birth on [redacted] college transcripts and birth certificate and for wearing on [redacted] uniform Airborne and Air Assault Badges [redacted] was never awarded. Finally [redacted] DD-214 indicated [redacted] was separated from military service after two years for [redacted].

OI interviewed [redacted], MOPH, who stated [redacted] publically portrayed [redacted] as a decorated war veteran and provided false documentation to MOPH in support of [redacted] application to become a member. [redacted] provided OI with copies of the documents [redacted] alleged [redacted] falsified, which included a NARA Form 13164 (Information Releasable Under the Freedom of Information Act) and a letter from the NARA, Textual Service Division. A review of these documents by [redacted] revealed that they were not created by NARA.

Referral to Veterans Administration, Office of Inspector General, Criminal Investigations Division (VA-OIG-CID)

OI contacted VA-OIG-CID and provided all documentation obtained from [redacted]. VA-OIG-CID subsequently analyzed [redacted] complete VA [redacted] history and determined [redacted] submitted falsified documents to the VA to substantiate [redacted] eligibility for veteran's benefits. VA-OIG-CID further determined [redacted] received $6,647.61 in VA [redacted] benefits to which [redacted] was not entitled.

VA-OIG-CID interviewed [redacted] who admitted [redacted] made false statements, created false government documents, submitted those false documents to the VA, received VA [redacted] benefits [redacted] was not entitled to and falsely claimed [redacted] was awarded a Purple Heart and Silver Cross by the U.S. Army.

Coordination with U.S. Attorney's Office (USAO), [redacted]

On [redacted], 2011, VA-OIG-CID presented this case to the USAO for the [redacted]. A prosecutorial determination is pending.

Conclusion

This investigation is closed pending a prosecutorial determination and potential action by the USAO.

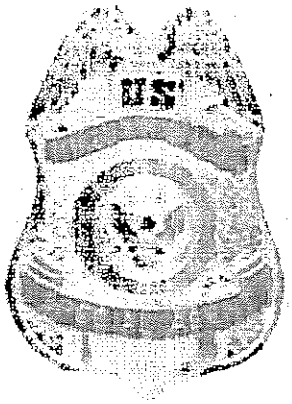
Investigation Number:	Case Title:
10-0011-I	Stolen Valor Veteran Record Fraud

OFFICE OF INSPECTOR GENERAL

OFFICE OF INVESTIGATIONS

REPORT OF INVESTIGATION:

11-0015-I



WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
11-0015-I	[redacted]	
Period of Investigation:	**Type of Report:**	**Distribution:**
July 2011 – February 2014	☐ Interim ☒ Final ☐ Supplemental	☒ Info Only ☐ Referred ☐ Closed to File

SUBJECT(S) OF INVESTIGATION

[redacted]

[redacted]

BASIS FOR INVESTIGATION

On July 11, 2011, [redacted], Security Specialist, Holdings Protection Team (HPT), National Archives and Records Administration (NARA), contacted the Office of Inspector General (OIG), Office of Investigations (OI), about allegations [redacted] and [redacted] stole historical records from [redacted] in Baltimore, MD.

The OI met [redacted] staff, HPT staff, and Federal Bureau of Investigation (FBI) agents to review historical records the Baltimore City Police found in [redacted] and [redacted] possession during their arrest. As a result, the OI took custody of seven historical records to determine if they were federal records stolen from NARA, and the FBI requested the OI join their investigation to assist in a search warrant at [redacted] residence in New York City.

ALLEGED VIOLATIONS

18 U.S.C. § 668: Theft of Major Artwork

18 U.S.C. § 371: Conspiracy to Commit Theft of Major Artwork

Prepared by: [redacted]	Signature: [redacted]	Date of Report: May 28, 2014
Approved by: AIGI Matthew Elliott	Signature:	

NARA - OIG Form OI 212 (02/2013)

Office of Inspector General
National Archives and Records Administration

REPORT OF INVESTIGATION (Continued)

RESULTS OF INVESTIGATION

This joint investigation substantiated [redacted] and [redacted] conspired to steal historical records from NARA and other public and private collections. During this investigation [redacted] and [redacted] admitted they used various techniques to steal historical records including concealing them inside sport coats and other outerwear modified to contain hidden pockets. To conceal their thefts, [redacted] and [redacted] removed markings and inventory control notations from the stolen records and stole or destroyed finding aids from victim institutions.

[redacted] and [redacted] stole seven reading copies[1] of Presidential speeches from the Franklin D. Roosevelt Library and Museum (LP-FDR) in Hyde Park, NY. Although [redacted] sold four of the speeches to a collector, the OI and FBI recovered all seven that in total were valued over $335,000. During earlier visits without [redacted] stole at least eight additional items from the LP-FDR including letters and invitations.

Although [redacted] did not recall what specifically [redacted] stole from the Herbert Hoover Presidential Library and Museum (LP-HH) in West Branch, IA, the OI established evidence [redacted] removed at least 2 museum holdings.

Because of this investigation, the OI and FBI released over 10,000 historical items to public and private victims, including 718 to the LP-FDR and 46 to the LP-HH

The Department of Justice (DOJ) accepted this case for prosecution and [redacted] and [redacted] pleaded guilty to theft of major artwork and conspiracy. The U.S. District Court for the District of Maryland (Court) sentenced [redacted] to 7 years in prison followed by 3 years of supervised release, and ordered [redacted] to pay restitution and forfeit to the FBI all evidence seized from [redacted] residence during both search warrants. The Court sentenced [redacted] to 12 months and one day in prison followed by 2 years of supervised release.

INVESTIGATIVE SUMMARY

FBI Search Warrants

On July 12, 2011, the FBI and OI executed a search warrant at [redacted] residence, and the FBI seized thousands of evidence items including documents and ephemera.[2] The FBI released 9,013 of the seized items to the OI for processing, examination, and protection.

On August 2, 2011, while the FBI and OI executed a second search warrant at [redacted] residence, [redacted], accompanied by [redacted] defense counsel, identified additional stolen records. As a result, the FBI seized an additional 1,185 items and released them to the OI.

[1] "Reading copies" are the actual copies of the speeches from which President Roosevelt read and contain edits and handwritten additions made by him, and bear his signature.
[2] Ephemera - A class of collectable items not originally intended to last for more than a short time, such as tickets, menus, invitations, posters, postcards, or labels.

REPORT OF INVESTIGATION (Continued)

OI and NARA Review of Seized Evidence

The OI assisted by staff from Archival Operations-Washington, DC, and the Office of Presidential Libraries (LP), processed, examined, protected, and cataloged 10,198 items seized from both search warrants. Through archival examinations, contact with suspected victim institutions, and interviews of [redacted] and [redacted], the OI identified the likely origins of the seized items - disposition of the items is detailed later in this report.[3]

OI Computer Forensics

The OI examined two laptop computers and various removable electronic media the FBI seized from [redacted] residence. The examinations established probable cause for a search warrant on [redacted] private email accounts that revealed [redacted] and [redacted] sent emails to each other about "augmentation" and "weaseling," and referred to each other as "W1" and "W2." Further analysis linked [redacted] and [redacted] research list, internet searches, research communication, and co-conspirator communication with travel to victim institutions, and corroborated information identifying known dealers who had purchased historical records from [redacted]. From the email accounts, the OI also discovered a spreadsheet named "Freedom Collection" containing a list of over 180 stolen documents that included information on [redacted] efforts to research the documents.

OI Interviews of [redacted]

Twice at Archives II, the OI interviewed [redacted] with [redacted] defense counsel present. During the interviews, [redacted] reviewed over 1,000 items seized from [redacted] residence and assisted the OI and FBI in determining the origin of many of the stolen historical records. [redacted] also provided the following information:

[redacted] corroborated that [redacted] and [redacted] used the "Freedom Collection" spreadsheet to reference their significant stolen historical records. The spreadsheet contained: the author and date of the record; the collection it originated from; the existence of a museum card catalog; and the existence of any microfilm or other finding aid related to the historical record. [redacted] also confirmed [redacted] and [redacted] referred to themselves as "Weasel 2" and "Weasel 1" respectively, and explained they wrote "W2" in pencil on certain historical records to track thefts involving [redacted].

[redacted] admitted that from December of 2010 through July of 2011, [redacted] conspired with [redacted] to steal historical records from NARA and other institutions. [redacted] stated they targeted institutions they believed contained rare and valuable historical records, and, under [redacted] direction, [redacted] used the internet to find valuable historical collections to target. They compiled lists of famous and historical people, frequently noting the approximate market value of records those individuals had authored. They intentionally looked for presidential ephemera such as invitations, menus, and tickets because institutions usually did not catalog or inventory those items.

[3] None of the seven historical records initially seized by the Baltimore City Police were NARA records.

REPORT OF INVESTIGATION (Continued)

admitted they visited numerous institutions, often posing as researchers, and accessed collections of historical records they thought were of significant value. When visited certain institutions, also used aliases to conceal identity. and used various techniques to steal including concealing records inside their sport coats and other outerwear a tailor had modified to contain hidden pockets. To conceal their thefts, and stole card catalog entries and other finding aids. After their thefts, they used sandpaper and other abrasive materials to remove markings or inventory control notations on some of the records – a process they called "surgery."

OI Interviews of

With the permission of defense counsel, the OI interviewed at apartment , and at . also agreed to assist the OI and the FBI in identifying victim institutions for approximately 388 separate pieces of orphaned[4] ephemera. During the interviews, provided the following information:

began stealing historical records in 2000, when stole 12-24 pieces of presidential ephemera from a private institution. never returned to steal from that institution because the institution organized their collection and referenced their ephemera records on their website. This deterred from stealing because did not want to steal historical records that were traceable back to a source institution. Also in 2000, purchased a computer to browse websites and look for other historical institutions to victimize.

Advance from

In 2005, Landau received . Before met , used money to visit and steal from NARA facilities and other public and private institutions.

Thefts from NARA Facilities

LP-HH

visited the LP-HH once while conducting research for in 2005. During the visit, conducted research and stole approximately 12-24 historical records from boxes the LP-HH staff served in their research room. These records consisted of several train menus related to trips President Hoover took to Palo Alto, and ephemera related to President Hoover's fraternity and a school Hoover attended. could not recall specific information about the other stolen records.

[4] Historical records or ephemera with no known origin because they were not officially accessioned, supported by a finding aid, or listed in a catalog collection.

REPORT OF INVESTIGATION (Continued)

[redacted] could not recall the number of boxes [redacted] accessed, but remembered they were ready when [redacted] arrived. The LP-HH allowed [redacted] to bring a folder into the research room while reviewing the presidential material. [redacted] could not remember how many LP-HH staff members were in the research room, but believed even with staff present [redacted] could have stolen the records. [redacted] explained that while sitting at [redacted] research desk, it was easy to slip stolen records into [redacted] folder without detection. Also, LP-HH staff did not check [redacted] research materials before [redacted] entered or departed the research room.

LP-FDR

[redacted] visited the LP-FDR at least 6 times - 4 times alone and twice with [redacted] On [redacted] 4 unaccompanied visits, [redacted] claimed [redacted] stole approximately 12 historical records. [redacted] only remembered one of the items [redacted] stole and described it as the "Bertie" letter. The OI determined this letter had been seized from [redacted] apartment and LP-FDR staff confirmed it was a NARA holding.

While [redacted] reviewed NARA records, the LP-FDR staff allowed [redacted] to place [redacted] research folder on [redacted] desk and did not search [redacted] folder before [redacted] entered or departed the research room. [redacted] noted the library received a lot of visitors and researchers and it appeared short staffed. When the LP-FDR staff pulled materials for other researchers, they routinely left the research room unattended. [redacted] felt these factors made it easier for [redacted] to steal from the LP-FDR.

On their first visit together to the LP-FDR, [redacted] and [redacted] posed as researchers to gather information on FDR's inaugural speeches and addresses from the FDR Master Speech File. During their second trip to LP-FDR, they stole the items they had identified during their first visit [redacted] and [redacted] intentionally requested numerous boxes from the Master Speech File to make it difficult for the research room staff to determine if any records were missing. They used their modified jackets to hide and steal historical records from the library. [redacted] recalled it was a busy day in the research room and staff preoccupation with other researchers made it easier to steal the speeches and inaugural addresses.

[redacted] Visits to NARA Facilities Prior to [redacted] Involvement with [redacted]

Harry S. Truman Library (LP-HST)

[redacted] visited the LP-HST once in the 1990's and once as part of a [redacted] in 2007. Although [redacted] believed it was easy to steal from the LP-HST in the 1990's, [redacted] did not steal because the library served [redacted] records stamped with a LP-HST mark. At that time, [redacted] considered the records defaced which deterred [redacted] from stealing. [redacted] noted that a significant amount of time passed between [redacted] two visits to the LP-HST and that during that timeframe, [redacted] had begun stealing "stamped" records for [redacted] collection. During [redacted] second visit, [redacted] planned to steal historical records, but learned the library no longer served original, stamped historical records to researchers. During both of [redacted] visits, the LP-HST staff did not inspect [redacted] belongings when [redacted] entered and departed the research room.

REPORT OF INVESTIGATION (Continued)

Dwight D. Eisenhower Library (LP-DDE)

[redacted] visited the LP-DDE only once as part of [redacted] book tour. The LP-DDE staff gave [redacted] a tour of the library, but [redacted] did not conduct research and never had access to original historical records. However, [redacted] admitted that [redacted] saw some interesting clothing and ephemera [redacted] would have stolen if staff had left [redacted] alone with the items.

John F. Kennedy Library (LP-JFK)

[redacted] visited the LP-JFK once in 2010. While conducting research, [redacted] discovered an original invitation to President Eisenhower's Inaugural Ball sent to John F. Kennedy mixed in with photocopies LP-JFK staff had served [redacted]. [redacted] was so excited about the discovery that [redacted] told the LP-JFK staff, but was later angry with [redacted] for reporting it because [redacted] wanted to steal the invitation.

Richard M. Nixon Library (LP-RN)

[redacted] visited the LP-RN once in 2004 or 2005 before the library was officially part of NARA. The LP-RN only served [redacted] photocopies, so there were not original records for [redacted] to steal.

Gerald R. Ford Library (LP-GRF)

[redacted] visited the LP-GRF in 2007 as part of [redacted]. [redacted] claimed [redacted] did not conduct research during this visit, nor did [redacted] steal historical records from the library.

Ronald Reagan Library (LP-RR)

[redacted] visited the LP-RR in 2005 and recalled library staff would not give [redacted] President Reagan's second inaugural address, because it was unavailable for public research. The LP-RR did serve [redacted] ephemera and [redacted] photocopied 200-300 pages. The LP-RR staff watched [redacted] closely preventing [redacted] from stealing any records.

REPORT OF INVESTIGATION (Continued)

Disposition of Material Seized from [redacted] Apartment to NARA Facilities

LP-FDR

The OI, with the assistance of the FBI, released 709 historical records to the LP-FDR including:

- The "Bertie" letter.
- Three reading copies of inaugural addresses from 1937, 1941, and 1945.
- Three invitations for the 1933 Inaugural, an Anniversary Ball, and an event held by Eleanor Roosevelt.
- 702 records consistent with other LP-FDR records, but not confirmed as missing from NARA holdings.

OI Interview of [redacted]

[redacted], LP-FDR, explained that at the time of the theft, the inaugural speeches were stored in approximately 80 archival boxes from the overall Master Speech File. In 2009, a contractor microfilmed this speech file, but did not create an index or reference list for the microfilmed file. Because the LP-FDR staff did not have a reference list or index, they served the original historical speeches to researchers instead of the microfilm.

[redacted] determined [redacted] visited LP-FDR 7 times alone and twice with [redacted], who used the alias [redacted]. The LP-FDR served [redacted] 466 boxes of records when [redacted] visited the library alone, and 38 boxes when [redacted] and [redacted] visited together. On the day of the theft, [redacted] and [redacted] sat in the back of the research room, which was crowded and extremely busy.

LP-FDR Internal Control Procedural Changes

Because of the OI and FBI joint investigation, the LP-FDR staff reviewed the microfilmed speech file and created an index guide and finding aid. The LP-FDR no longer serves researchers original historical records from the Master Speech File and the LP-FDR retired the original records from the Master Speech File to a secure location.

At the time of the thefts, the LP-FDR served researchers up to 15 boxes of records. Now, the LP-FDR serves researchers no more than 10 boxes at a time, and the LP-FDR allows each researcher to have only one box on the top shelf of their cart. The other 9 must remain on the bottom 2 shelves of their cart.

REPORT OF INVESTIGATION (Continued)

This investigation has also caused staff levels to change in the research rooms. During research hours, a minimum of two LP-FDR staff must be present in the research room. One staff member registers and assists researchers while the other staff member monitors the room. Prior to the thefts, only one staff member performed both functions.

LP-HH

The OI released 46 historical records to the LP-HH including:

- 2 tickets for the 1929 inauguration that were previously identified as missing from LP-HH museum holdings.
- 44 items consistent with LP-HH, records, but not confirmed as missing from NARA holdings.

Disposition of Material Seized from [redacted] Apartment to Non - NARA Victims

The OI and the FBI released:

- 7,705 historical records to 13 public institutions.
- 179 historical records to 5 private institutions.
- 265 historical records to 3 individual victims.
- 1,237 items to [redacted]
- 5 items to [redacted]

Because it would have been inappropriate to return the items to their original owner, the OI, [redacted] (B)(5) Per EOUSA [redacted] destroyed the remaining 52 items.

REPORT OF INVESTIGATION (Continued)

Disposition of Historical Records Recovered from Dealers

The OI and the FBI recovered 21 stolen historical records that [redacted] sold to 5 different dealers in the United States. The OI and the FBI returned 9 records to the LP-FDR; 10 records to five public institutions; and 2 records to a single victim.

The LP-FDR records recovered from a New York book dealer included:

- Reading copy of a 1941 address in connection with the Thirteenth Annual Awards Dinner of the Academy of Motion Picture Arts and Sciences, signed "Franklin D. Roosevelt."
- Reading copy of a 1941 broadcast, signed "Franklin D. Roosevelt."
- Reading copy of a 1941 radio address, signed "Franklin D. Roosevelt."
- Reading copy of a 1945 radio address, signed "Franklin D. Roosevelt."
- Bound copy of a 1936 address given by FDR in Chautaqua, NY.
- Letter on White House stationery from FDR to Mrs. Henry Morgenthau, Jr., dated January 10, 1940, and signed "Franklin D. Roosevelt," with envelope.
- Letter on White House stationery from FDR to Mrs. Henry Morgenthau, Jr., dated February 1, 1941, and signed "Franklin D. Roosevelt."
- Letter on White House stationery from FDR to Secretary of the Treasury and Mrs. Henry Morgenthau, Jr., dated February 5, 1941, and signed "Franklin D. Roosevelt."

Disposition of Historical Records Surrendered by [redacted] and [redacted]

[redacted]

On August 24, 2011, [redacted], with defense counsel present, surrendered to the OI, a framed sketch picture, a post card, and a catalog card. The OI and FBI determined [redacted] stole the three items and the OI returned them to a public institution.

REPORT OF INVESTIGATION (Continued)

[redacted]

On September 28, 2011, [redacted], through [redacted] defense counsel, surrendered to the OI an 1868 letter from Andrew Johnson, two catalog cards, a drawing, and an 1864 presidential pardon issued by Abraham Lincoln. The OI and FBI determined [redacted] and [redacted] stole the 1868 letter and catalog cards and the OI returned them to a public institution. The OI and FBI also determined [redacted] stole the drawing and the 1864 presidential pardon and the OI returned them to a private individual through [redacted] defense counsel.

On July 26, 2012, [redacted] surrendered to the OI, two 1865 Harper's Weekly newspapers. The OI determined [redacted] stole the newspapers and the OI returned them both to a bookstore.

Prosecution by the DOJ

[redacted]

On February 7, 2012, [redacted] pleaded guilty in U.S. District Court for the District of Maryland to one count of 18 U.S.C. § 668: Theft of Major Artwork; and one count of 18 U.S.C. § 371: Conspiracy.

On June 27, 2012, the Court sentenced [redacted] to 7 years in federal prison followed by 3 years of supervised release and ordered to pay restitution to three victims totaling $46,525.00. The Court ordered [redacted] to forfeit to the FBI, all evidence seized from [redacted] residence.

[redacted]

On October 27, 2011, [redacted] pleaded guilty in the U.S. District Court for the District of Maryland to one count of 18 U.S.C. § 668: Theft of Major Artwork; and one count of 18 U.S.C. § 371: Conspiracy.

On November 9, 2012, the Court sentenced [redacted] to 12 months and one day in federal prison followed by 2 years of supervised release.

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
12-0013-I	ART-Missing Eva Braun Original Home Movie Reels	
Period of Investigation: September 2011-October 2014	**Type of Report:** ☐ Interim ☒ Final ☐ Supplemental	**Distribution:** ☐ Info Only ☐ Referred ☒ Closed to File

SUBJECT(S) OF INVESTIGATION

N/A

BASIS FOR INVESTIGATION

On September 29, 2011, [redacted] Motion Picture Branch (RDSM), National Archives and Records Administration (NARA), notified the NARA Office of Inspector General (OIG), Office of Investigations (OI) that Eva Braun's original home movies she made of Hitler and high-ranking Nazi Government officials (original Eva Braun film)[1] have been missing from NARA for several years.

ALLEGED VIOLATIONS

18 U.S.C. § 641: Public Money, Property or Records

RESULTS OF INVESTIGATION

Based on conflicting and missing documentation, the OI could not determine the location or disposition of the original Eva Braun film. It remains missing. The most recent documentation demonstrating NARA likely had custody of the original Eva Braun film is dated June 1973, when NARA maintained motion picture holdings at Archives I.

[1] The original Eva Braun film corresponds to NARA item number 242.2 and consists of several reels of motion picture film.

Prepared by:	Signature:	Date of Report:
SA [redacted]	[redacted]	October 30, 2014
Approved by: Acting AIGI James Springs	James Springs	

REPORT OF INVESTIGATION (Continued)

The OI determined the most likely description of the missing original Eva Braun film is eight (8) reels containing a mixture of 16mm black/white and16 mm Agfacolor[2] brand and/or Kodak brand film totaling 9,167 feet in length. The color portions of the original Eva Braun film are likely silent reversals (O.R.S.K).[3]

In the 1990s, NARA staff systematically copied acetate films onto more stable film media due to "vinegar syndrome."[4] NARA staff then destroyed the original films without documenting their descriptions. There was no formal policy regarding the acetate film duplication project and the OI found no records indicating what particular films were destroyed.

In 1999, NARA staff could not locate the original Eva Braun film. In 2006, after numerous search efforts, NARA staff made the final determination that the original Eva Braun film was missing. In 2011, as the OI was actively investigating the theft of RDSM holdings, [redacted] made notification that the original Eva Braun film had been missing for years and requested that the OI investigate the disappearance. [redacted] said the original Eva Braun film was identified missing during the tenure of [redacted] predecessor.

Due to missing film inspection reports[5], NARA staff could not advise the OI when staff last handled the original Eva Braun film. The OI searched through surviving film inspection reports for information on the original Eva Braun film and found no reference.

The OI interviewed the current and three former RDSM Supervisory Archivists and seven additional current or former RDSM employees. The OI interviewed filmmakers who produced documentaries about the original Eva Braun film and interviewed personnel at non-NARA motion picture laboratories.

NARA staff and the OI asked non-NARA companies and institutions to search their holdings for the original Eva Braun film. NARA staff also queried NARA's offsite motion picture storage facility located in Lenexa, Kansas. These activities produced negative results.

The OI confirmed NARA maintains duplicates of the original Eva Braun film that appear to contain the complete content of the original Eva Braun film. NARA consistently provides these duplicates for researcher use and found no evidence that access was impacted.

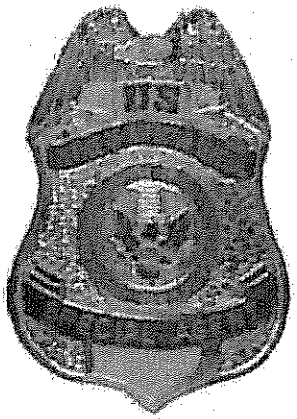
[2] Agfacolor was a series of color film products made by Agfa of Germany introduced in 1932. Agfacolor was originally a reversal film used for making slides, home movies, and short documentaries.
[3] O.R.S.K.: Original, Reversal, Silent, Color (Note: the film industry acronym utilizes the letter K - not C - to represent color.)
[4] "Vinegar syndrome," or acetate film base degradation, is a decay process leading to a pungent vinegar smell, shrinkage, embrittlement, and buckling of acetate film's gelatin emulsion. These conditions ultimately lead to the film's complete destruction.
[5] Film inspection reports are used by NARA staff to document the results of film element inspections. These reports detail the type and description of an inspected film element, along with the date and location where a film element was inspected. Such a report would potentially provide information to identify when, and by what film inspector, the missing Eva Braun film was last handled.

OFFICE OF INSPECTOR GENERAL

OFFICE OF INVESTIGATIONS

REPORT OF INVESTIGATION:

12-0022-I



WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
12-0022-I	Theft, Concealment and Destruction of Veterans' Records at the NPRC	
Period of Investigation: July 2012 – January 2014	**Type of Report:** ☐ Interim ☒ Final ☐ Supplemental	**Distribution:** ☐ Info Only ☒ Referred ☐ Closed to File

SUBJECT(S) OF INVESTIGATION

Former National Archives and Records Administration (NARA), National Personnel Record Center (NPRC), temporary student employees:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

BASIS FOR INVESTIGATION

On July 4, 2012, [redacted] NPRC, reported to the Office of Inspector General (OIG), Office of Investigations (OI) that approximately one cubic foot of veterans' records[1] from the NPRC had been discarded in a wooded area in Alton, IL. [redacted] explained that on July 3, 2012, [redacted], a private citizen, discovered the documents and contacted the NPRC. [redacted] collected some of the documents and showed them to [redacted] and an NPRC archivist. [redacted] and the archivist confirmed the documents were veterans' records from the NPRC, and immediately went to the area where [redacted] found them to take photographs and recover the additional records.

[1] A veteran's record or interfile refers to an official document or set of related documents intended for or from a veteran's Official Military Personnel File held at NPRC.

Prepared by: SA [redacted]	[redacted]	Date of Report: March 21, 2014
Approved by: AIGI Matthew Elliott	Signature:	

REPORT OF INVESTIGATION (Continued)

ALLEGED VIOLATIONS

18 USC § 641: [Theft of] Public money, property or records

18 USC § 2071: Concealment, removal, or mutilation generally [of Federal records]

18 USC § 1001: [False] Statements or entries generally

NARA Policies and Directives

RESULTS OF INVESTIGATION

A joint investigation with the Federal Bureau of Investigation (FBI) substantiated [redacted] stole 251 veterans' records from the NPRC and discarded them in a wooded area in Alton, IL.[2] An OI analysis of internal NPRC audits also revealed [redacted] removed, concealed, destroyed or attempted to destroy at least 3,002 additional veterans' records. The OI and FBI interviewed [redacted] who admitted [redacted] discarded the NPRC records recovered from the wooded area.

Investigative interviews and internal NPRC audits also substantiated [redacted] and [redacted] removed, concealed, destroyed or attempted to destroy at least 1,523 additional veterans' records. [redacted] admitted [redacted] removed and destroyed NPRC veterans' records and concealed records in the NPRC. [redacted] and [redacted] admitted they concealed records in the NPRC, but denied removing or destroying records.

[redacted] and [redacted] also showed the OI and FBI where they had concealed approximately 300 records[3] in the NPRC. The OI recovered the records and immediately released them to the NPRC for processing. The NPRC will continue efforts to process and re-file the recovered documents.

The OI also developed evidence [redacted] submitted falsified college transcripts to maintain [redacted] eligibility to participate in the Student Temporary Employment Program (STEP).[4]

The Department of Justice (DOJ) accepted this case for prosecution, and [redacted] and [redacted] pleaded guilty to one count each of misdemeanor theft of public records. Both were sentenced in Federal court to two years

[2] The NPRC reviewed the recovered documents and identified the personal data of 132 veterans not known to be deceased. The NARA Office of General Counsel notified the 132 veterans and offered credit monitoring services. To date, there is no evidence any of those 132 veterans were impacted by the potential disclosure of their personal information. However, one veteran did need a document recreated.

[3] A "record" may consist of one or more pages, and these materials consisted of mixed, potentially related documents. Therefore, the OI could not immediately determine the actual number of records recovered.

[4] STEP provided students in high schools, colleges, trade schools and other qualifying educational institutions with paid opportunities to work in Federal agencies while completing their education. Since this investigation was initiated, the Office of Personnel Management replaced STEP with the Pathways Program.

REPORT OF INVESTIGATION (Continued)

probation. The DOJ placed [redacted] in pre-trial diversion, but declined to prosecute [redacted] and [redacted]. NARA terminated [redacted] from federal service, and the other four employees resigned.

In conjunction with this investigation, the OIG also issued two letters to NARA management related to veterans' record issues at the NPRC and NPRC's management of its student workforce.[5]

INVESTIGATIVE SUMMARY

OI Interview of [redacted]

[redacted] stated [redacted] met with [redacted] who had collected a variety of military documents from a wooded area near [redacted] office in Alton, IL. The documents included casualty reports, separation reports, and medical documents with NPRC Finding Aid Reports (FARs) attached to them. The FARs suggested these documents had come from the NPRC. [redacted] stated the documents were records from the U.S. military that should have been filed into existing Official Military Personnel Files (OMPF) held at the NPRC. Many of the documents included personally identifiable information [redacted] reported NPRC staff reviewed the FARs attached to the recovered documents, and determined the documents had been assigned to [redacted] for filing.

Joint Interviews of [redacted]

The OI and FBI interviewed [redacted] after NPRC staff determined the recovered records had been assigned to [redacted] for filing. The OI, FBI and DOJ interviewed [redacted] a second time after DOJ accepted the case for prosecution.

[redacted] admitted [redacted] removed the records in a personal bag, stored the bag in [redacted] personal vehicle, and after a period of time dumped the records in the woods. [redacted] also stated that between May and July 2012, [redacted] removed records from the NPRC approximately 5 to 10 times and then destroyed them. [redacted] admitted [redacted] dumped 2 plastic bags containing less than 200 records in [redacted] home trash and later dumped 2 more plastic bags containing approximately 175-280 in [redacted] home trash. [redacted] also admitted [redacted] intentionally misfiled 200-300 records. Further, [redacted] also admitted [redacted] falsely certified on NPRC batch sheets[6] that [redacted] properly filed interfiles assigned to [redacted] Instead [redacted] removed and destroyed, misfiled, or hid the records to avoid the work necessary to properly file them.

To remove records, [redacted] first hid them in [redacted] locker or in bins within the NPRC. [redacted] then hid the records under [redacted] shirt or placed them in a personal bag, walked past NPRC security, and put the records into [redacted] personal vehicle. [redacted] then drove them offsite for disposal [redacted] stated [redacted] coached [redacted] on how to

[5] Management Letters No. 12-18, *Veteran Records Issues*, dated July 30, 2012, and No. 13-04, *Vulnerabilities in Managing the Student Workforce at the National Personnel Records Center*, dated December 4, 2012.

[6] Batch sheets are documents that list a range of NPRC registry numbers associated with veterans' records assigned to NPRC employees for filing. Batch sheets have signature blocks where employees certify they properly filed the veterans' records.

REPORT OF INVESTIGATION (Continued)

hide records within the NPRC or remove and destroy them. Finally, [redacted] stated [redacted] had also been destroying records since May 2012.

[redacted] also showed the OI and FBI where [redacted] had concealed approximately 200 records in the NPRC. The OI recovered the records and immediately released them to the NPRC for processing.

Joint Investigation of [redacted]

Evidence [redacted] Intentionally Misfiled Veterans' Records

The OI and FBI interviewed [redacted] who stated [redacted] had heard about this investigation and that it was about "stashing interfiles." When asked if [redacted] hid interfiles, [redacted] stated, "I used to do that, but only twice." [redacted] would not provide additional detail about what [redacted] meant, and only explained that [redacted] could have accidentally misfiled Navy records into Army records. Finally, [redacted] said the last time [redacted] did refiles was in December 2011.

An NPRC employee told the OI and FBI they had spoken with [redacted] following [redacted] resignation from the NPRC. They stated [redacted] told them "I sure wish I hadn't told those guys how to hide the interfiles." The employee stated [redacted] was referring to the fact that [redacted] taught [redacted] and [redacted] how to hide records at the NPRC.

Evidence [redacted] Submitted Falsified Transcripts to NARA

The OI evaluated transcripts [redacted] submitted to maintain [redacted] eligibility to participate in the STEP program and subsequently established evidence [redacted] had falsified those transcripts.

Joint Interviews of [redacted]

The OI and FBI interviewed [redacted] after [redacted] alleged [redacted] had also removed and destroyed veterans' records. The OI, FBI and DOJ interviewed [redacted] a second time after DOJ accepted the case for prosecution.

[redacted] admitted that while employed at the NPRC between November 2011 and March 2012, [redacted] removed and destroyed records on at least two occasions. [redacted] hid the records under [redacted] clothing, walked past NPRC security, and put the records in [redacted] personal vehicle. [redacted] then burned the records in a fireplace at [redacted] residence.

Additionally, [redacted] admitted [redacted] intentionally filed multiple veterans' records into a single, unrelated OMPF. [redacted] explained that [redacted] inserted a correct record into an OMPF, but also included an unrelated veterans' record from [redacted] batch. [redacted] told the OI this practice essentially reduced [redacted] work load by half. [redacted] stated [redacted] hid or misplaced approximately 100 to 300 records within the NPRC. Finally, [redacted] admitted [redacted] falsely certified [redacted] had properly filed veterans' records, which [redacted] had instead misfiled or destroyed.

REPORT OF INVESTIGATION (Continued)

[redacted] stated [redacted] showed [redacted] how to hide or dispose of records to avoid work. [redacted] told [redacted] to place records into a record redistribution bin to avoid completing the assignment. [redacted] showed [redacted] how to double file[7] records, and [redacted] knew [redacted] had removed records from the NPRC. [redacted] didn't notify NPRC management because of peer pressure, and because [redacted] had himself hidden and destroyed records.

[redacted] also showed the OI and FBI where [redacted] had concealed approximately 100 records in the NPRC. The OI recovered the records, and immediately released them to the NPRC for processing.

NPRC Employee Audits

To identify additional documents that may have been concealed, removed or destroyed, the NPRC audited interfile work assigned between April 2011 and July 2012 to [redacted], [redacted], and [redacted]. An OI analysis of the audit results showed:

- [redacted] signed batch sheets for 4,741 records, and 3,002 are missing.
- [redacted] signed batch sheets for 1,144 records, and 813 are missing.
- [redacted] signed batch sheets for 806 records, and 129 are missing.

The NPRC also audited interfile work assigned to all NPRC employees during the same time frame. NPRC management found [redacted] and [redacted] percentage of missing files were significantly above the NPRC average error rate, and forwarded the information to the OI. An OI analysis of the audit results showed:

- [redacted] signed batch sheets for 858 records, and 212 are missing.
- [redacted] signed batch sheets for 1,521 records, and 369 are missing.

The NPRC audit also identified a sixth student employee who signed batch sheets for 435 records, and 93 are missing. However, the employee resigned and refused a request to be interviewed. The OI and FBI did not find any additional evidence the former employee concealed, removed or destroyed records, so the OI and FBI did not present the individual to the DOJ for potential prosecution.

[7] Double or triple filing is when an NPRC employee files multiple unrelated veterans' records with a properly filed veterans' record.

REPORT OF INVESTIGATION (Continued)

Joint Interviews of [redacted] and [redacted]

Representatives from the OI, FBI and DOJ jointly interviewed [redacted] and [redacted].

[redacted]

[redacted] admitted [redacted] intentionally misfiled about 80 veterans' records on only one occasion during [redacted] two and half year employment at the NPRC.

[redacted]

[redacted] admitted that while employed at the NPRC between May and July 2012, [redacted] intentionally misfiled records by placing them into incorrect veteran OMPFs or hiding them under filing cabinets.

Investigative Activity Conducted Exclusively by the FBI

Although this was a joint investigation with the FBI, the FBI conducted some activity independent of the OI. This investigative summary does not detail that activity.

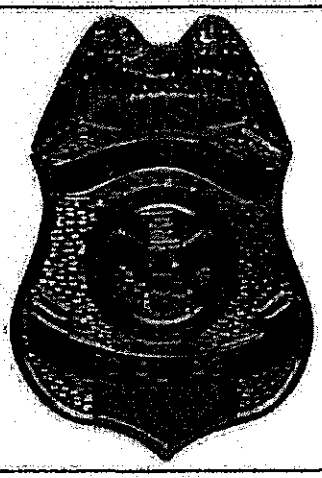
Prosecution by the DOJ

[redacted] pleaded guilty in the U.S. District Court for the Eastern District of Missouri to one misdemeanor count of 18 U.S.C. § 641: [Theft of] Public money, property or records. [redacted] was sentenced to two years probation.

[redacted] pleaded guilty in the U.S. District Court for the Eastern District of Missouri to one misdemeanor count of 18 U.S.C. § 641: [Theft of] Public money, property or records. [redacted] was sentenced to two years probation.

The U.S. Attorney's Office for the Eastern District of Missouri placed [redacted] in pretrial diversion,[8] and declined to prosecute [redacted] and [redacted].

[8] Pretrial diversion is an alternative to prosecution which seeks to divert certain offenders from traditional criminal justice processing into a program of supervision and services administered by the U.S. Probation Service. Participants who complete the program will not be charged or, if charged, will have the charges against them dismissed; unsuccessful participants are returned for prosecution.



OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

REPORT OF INVESTIGATIONS

Case Number: 13-0001-I

WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
13-0001-I	Customs Collector for the Port of Philadelphia, 1806	
Period of Investigation:	**Type of Report:**	**Distribution:**
October 2008-July 2014	☐ Interim ☒ Final ☐ Supplemental	☐ Info Only ☐ Referred ☒ Closed to File

SUBJECT(S) OF INVESTIGATION

N/A

BASIS FOR INVESTIGATION

On October 6, 2008, the National Coalition for History (NCH) reported to the National Archives and Records Administration (NARA), Office of the Inspector General (OIG), Office of Investigations (OI), that an 1806 document signed by former Revolutionary War General Peter Muhlenberg (Muhlenberg Document) was for sale on eBay by [redacted] The Muhlenberg Document details articles furnished for the use of a revenue boat in the port of Philadelphia.

ALLEGED VIOLATIONS

18 U.S.C. § 641 Embezzlement and Theft; Public Money, Property or Records

RESULTS OF INVESTIGATION

This investigation was delayed due to staff changes within the OI.

[redacted], archivist, NARA-Mid Atlantic Region (RE-PA) reviewed the eBay sale listing and stated [redacted] opinion was the Muhlenberg Document is a Federal record that was never accessioned into NARA's holdings. If NARA acquired the Muhlenberg Document, RE-PA would place it in the files of the Revenue Cutter Service in the Records of the United States Coast Guard (Record Group 26).

In order to determine information related to the Muhlenberg Document, the OI subpoenaed the eBay/Paypal Production Team (eBay/Paypal) for records associated with the following sale: [redacted] eBay item [redacted] Due to a lack of response from eBay/Paypal, the OIG Legal Counsel contacted eBay/Paypal and was told the records relating to the sale of the Muhlenberg Document no longer exist.

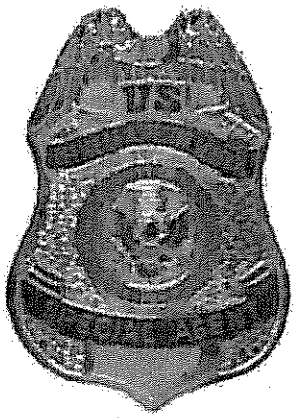
Prepared by:	Sign	Date of Report:
IA [redacted]	[redacted]	10/22/2014
Approved by:	**Signature:**	

OFFICE OF INSPECTOR GENERAL

OFFICE OF INVESTIGATIONS

REPORT OF INVESTIGATION:

13-0003-I



WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
13-0003-I	Missing Items from the LP-JFK	
Period of Investigation:	**Type of Report:**	**Distribution:**
May 2012 – January 2014	☐ Interim ☒ Final ☐ Supplemental	☐ Info Only ☒ Referred ☐ Closed to File

SUBJECT(S) OF INVESTIGATION

N/A

BASIS FOR INVESTIGATION

On May 11, 2012, [redacted], Holdings Protection Team (HPT), National Archives and Records Administration (NARA) referred to the Office of Inspector General (OIG), Office of Investigations (OI) a report that holdings used in a 2006 museum exhibit were missing from the John F. Kennedy Presidential Library and Museum (LP-JFK).

ALLEGED VIOLATIONS

N/A

RESULTS OF INVESTIGATION

LP-JFK staff conducted an initial search and found two audiovisual holdings originally reported as missing. Through several additional searches, LP-JFK staff found three complete textual holdings and three partial textual holdings. LP-JFK management also believes they may have found an additional two holdings. The OI found no evidence 15 holdings currently identified as completely or partially missing from LP-JFK were stolen.

The loan documentation for a 2006 transfer of holdings between the LP-JFK library and museum was incomplete and inaccurate, and the missing items were part of that loan. As a result of this incident, [redacted], LP-JFK, initiated new policies and procedures to track holdings loaned between the library and museum. In addition, [redacted] increased access controls over the secure cage holding high value items. The LP-JFK staff will continue their efforts to locate the missing holdings.

Prepared by:	Signature:	Date of Report:
SA [redacted]	[redacted]	February 21, 2014
Approved by: AIGI Matthew Elliott	**Signature:**	

NARA - OIG Form OI 212 (02/2013)

Office of Inspector General
National Archives and Records Administration

REPORT OF INVESTIGATION (Continued)

INVESTIGATIVE SUMMARY

Initial Discovery Items Were Missing from 2006 Exhibit

On April 19, 2012, [redacted], LP-JFK, searched for a NARA holding in the LP-JFK valuables collection.[1] During that search, [redacted] found an old withdrawal sheet with an attached photocopy of a letter from John F. Kennedy to Rose Kennedy. [redacted] determined that the original letter was missing from its assigned location within Box 37.[2] [redacted] told [redacted] that the withdrawal sheet indicated the original letter had been removed from the valuables collection in April 2006 and transferred to the LP-JFK museum for the Rose Kennedy exhibit.

LP-JFK Search for Missing Exhibit Items

OI Interview of [redacted]

After learning about the missing letter [redacted] initiated a search within the valuables collection to locate the missing holding. During that initial search, LP-JFK staff found additional copied withdrawal sheets for other holdings removed from the Rose Kennedy Personal Papers for the 2006 exhibit. [redacted] then initiated a full search of all 35 boxes in the Rose Kennedy Personal Papers.

[redacted] stated [redacted] was initially unable to locate any transfer documentation for the 2006 Rose Kennedy exhibit, so [redacted] had the museum registrar search the museum files. The museum registrar located a transfer document that indicated the former LP-JFK [redacted], received the exhibit items when they were transferred back to the library collection in 2006. [redacted] explained that in 2006, the LP-JFK had different procedures for internal loans between the library and the museum. Additionally, [redacted] noted that when [redacted] became [redacted], [redacted] found significant deficiencies in holdings maintenance and re-filing.

OI Interview of [redacted]

The OI showed [redacted] museum loan documentation that indicated [redacted] accepted the returned exhibit items featured in the 2006 Rose Kennedy exhibit at the museum [redacted] didn't recall the 2006 Rose Kennedy exhibit. However, [redacted] recalled viewing two items missing from the exhibit in the caged area prior to [redacted] retirement.

[1] Valuable items are removed from the open collection and placed under restricted access. For documentary materials, the valuable items are photocopied by NARA staff and the originals are placed in separate folders and locked in a secured cage area. Once placed in the cage area, the items are labeled to indicate their assignment to the valuables collection within the LP-JFK. The photocopies are placed in the open collection and made available for service to researchers. The valuables collection is not served to researchers.

[2] Rose Kennedy Papers, Box 37, includes valuable letters, postcards, report cards, and drawings from 1918-1928.

REPORT OF INVESTIGATION (Continued)

[redacted] explained that when items were returned from exhibits [redacted] would give them to a LP-JFK staff member for re-filing. [redacted] further noted the items from the 2006 Rose Kennedy exhibit would probably only fill a single file folder and most likely were all together in a single archival box when they were returned to the reference section for re-filing. [redacted] also explained some library holdings have been relocated due to a recent fire. Finally, [redacted] confirmed [redacted] never removed any folders or documents from LP-JFK.

Current Number of Textual Holdings Potentially Missing from the 2006 Rose Kennedy Exhibit

According to a summary of 20 textual holdings LP-JFK management believes may have been included in the 2006 exhibit, LP-JFK personnel found 3 complete documents; found 3 partial documents; and possibly found 2 complete documents. However, 12 complete documents remain missing (Exhibit 1).

LP-JFK Policy Changes to Strengthen Holdings Protection

Because of this incident, [redacted] has implemented procedural changes to improve how the library tracks internal loans to the museum and to limit access to the secure cage.

Policy Change for Internal Loan Process

[redacted] assigned two LP-JFK employees as the primary points of contact for all internal document loan requests. Both employees are responsible for managing all internal loans and transfers between the library and the museum. The policy addresses six key factors that comprise the transfer of archival materials for exhibits. Those factors are the Initial Request, Transfer Preparation (Finding/Citing Documents), Final Transfer Preparation (Preparing Documents for Transfer), Transfer of Documents, Return of Documents, and Missing Withdrawn Documents. [redacted] trained all LP-JFK staff on the new policies and procedures and believes the changes will improve the chain of custody for archival holdings loaned between the library and museum.

Policy Change for Access to the Cage

Before this incident, as many as seven LP-JFK staff members had unescorted access to the secure cage. [redacted] has since reduced cage access to two employees. [redacted] are now the only two employees with access to the cage area and [redacted] requires both employees be present when the cage is accessed. [redacted] also implemented a sign-in log for the cage which requires [redacted] to document (1) the purpose for access, (2) the time spent in the cage, and (3) if archival holdings were removed from the cage or re-filed.

EXHIBIT LIST

Exhibit Number	Description
1	Document provided by [redacted] entitled "Status of All Documents Used in the Fall 2006 Rose Kennedy Exhibit (Based on 8/9/2006 Document, "Temporary Transfer to Museum for Exhibit")"

Case Number:	Case Title:
13-0003-I	Missing Items from the LP-JFK

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

REPORT OF INVESTIGATIONS

Case Number: 13-0009-I

WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
13-0009-I	ART – 1865 Custer Weekly Effective Report	
Period of Investigation: 18MAR2013 – 23SEP2014	**Type of Report:** ☐ Interim ☒ Final ☐ Supplemental	**Distribution:** ☐ Info Only ☐ Referred ☒ Closed to File

SUBJECT(S) OF INVESTIGATION

N/A

BASIS FOR INVESTIGATION

On March 12, 2013, [redacted], contacted the National Archives and Records Administration (NARA), Office of the Inspector General (OIG), Office of Investigations (OI), Archival Recovery Team (ART) to report [redacted] of a historical document that was listed on the OIGs missing documents webpage. The historical document was a Weekly Station and Effective Force Report of the 2nd Calvary, dated October 2, 1865. The document was signed by Major General George Custer.

ALLEGED VIOLATIONS

18 U.S.C. § 668: Theft of Major Artwork
18 U.S.C. § 2071: Concealment, Removal, or Mutilation Generally

RESULTS OF INVESTIGATION

This investigation was unable to identify the person(s) responsible for the removal and theft of the historical record from NARA's holdings. The OI recovered the missing historical record through [redacted] after it was [redacted] a private collector from New York. The OI interviewed [redacted] and determined that [redacted] purchased the historical record in 2007 from [redacted] for $5,000. Through additional interviews with [redacted] staff and other private collectors, the OI determined that the historical record was sold to [redacted] by [redacted] The OI was unable to trace additional sales and purchasing information for the historical record because [redacted] failed to collect paperwork documenting [redacted] purchase. The OI conducted subsequent interviews of individuals that [redacted] believed had sold [redacted] the stolen record but was unable to substantiate [redacted] claim. In addition, the OI conducted additional interviews of known dealers in the region but found no evidence to further this investigation.

Prepared by:	Signature	Date of Report:
Special Agent [redacted]	[redacted]	10OCT2014
Approved by:	**Signature**	
[redacted]	[redacted]	

REPORT OF INVESTIGATION (Continued)

This investigation was not presented to the Department of Justice (DOJ) for prosecution based on insufficient documentary evidence in support of investigative findings.

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
13-0016-I	Questionable Acquisition	
Period of Investigation: July 2013 – April 2014	**Type of Report:** ☐ Interim ☒ Final ☐ Supplemental	**Distribution:** ☐ Info Only ☐ Referred ☒ Closed to File

SUBJECT(S) OF INVESTIGATION

[redacted]
National Archives and Records Administration (NARA)

BASIS FOR INVESTIGATION

In 2012, NARA contractor [redacted] - subcontracted [redacted] to perform a [redacted] assessment [redacted] assessment) of [redacted] for NARA's Online Public Access (OPA) system – a public facing component of NARA's Electronic Records Archive (ERA). NARA subsequently awarded [redacted] a contract to implement the recommendations from [redacted] assessment.

On June 3, 2013, the NARA, Office of Inspector General (OIG), Office of Audits (OA), reported to the NARA OIG, Office of Investigations (OI), allegations from [redacted]. [redacted] alleged [redacted] had [redacted] perform the assessment free of charge and without a contract, with the promise of future NARA contracts.

ALLEGED VIOLATIONS

5 C.F.R. Part 2635, Standards of ethical conduct for employees of the Executive branch

RESULTS OF INVESTIGATION

The OI reviewed NARA contract [redacted] but found no reference to the [redacted] assessment. As a result, the OI reviewed several other [redacted] contracts and interviewed [redacted] contractors and NARA staff from the Office of Acquisitions (BCN) and Office of Information Services (IS).

Prepared by: SA [redacted]	Signature:	Date of Report: February 3, 2016~~July 7, 2014~~
Approved by: Acting AIGI James Springs	Signature:	

REPORT OF INVESTIGATION (Continued)

The interviews and contract reviews revealed [redacted] conducted the assessment and [redacted] billed NARA $[redacted] under contracts [redacted] and [redacted]. NARA also awarded [redacted] a follow-on contract [redacted] to conduct work related to the findings in their assessment. The follow-on contract was reviewed and approved by BCN and the General Counsel's Office.

Review of NARA Contract Files

The OI reviewed NARA contract [redacted][1] and found that although the contract was an ERA support contract, the Statement of Work made no mention of OPA. The OI also reviewed NARA contract, [redacted][2] and found a technical direction letter requesting the [redacted] assessment. The OI also reviewed the files for both contracts, but found no invoices from [redacted] or [redacted] billing NARA for work related to the [redacted] assessment.

OI Witness Interviews

Interview of [redacted]

Prior to NARA, [redacted] was employed at [redacted] where [redacted] contracted [redacted] to perform work similar to the assessment. [redacted] believed [redacted] is one of few vendors experienced in evaluating [redacted]. In [redacted] experience, other vendors have expertise with only one particular [redacted]. After [redacted] told [redacted] NARA needed an assessment, [redacted] subcontracted with [redacted] to perform the work.

At the time of [redacted] interview, OPA was about to reach its implementation and maintenance phase and NARA intended to release a Request for Quote (RFQ) to compete this phase because it was outside the scope of the current [redacted] contract. [redacted] expected that [redacted] would bid for the work.

Interview of [redacted], *NARA*

[redacted] told the OI that the NARA Office of Information Technology decided to complete an assessment after several meetings between IS and BCN staff. [redacted] wanted to complete an assessment under the current [redacted] contract, but BCN told him that was not possible. [redacted] also spoke with [redacted] NARA [redacted], to determine if NARA could perform the work, but [redacted] told [redacted] NARA did not have the necessary specialized experience.

[1] [redacted] PMO was responsible for the oversight of the development of the ERA system.

[2] [redacted]

REPORT OF INVESTIGATION (Continued)

While looking for a subcontractor, [redacted] Program Manager, asked [redacted] several times what contractors [redacted] thought were capable of completing an assessment. [redacted] told [redacted] that [redacted] had positive prior experience with [redacted] at [redacted]. However, [redacted] never directed [redacted] to contract with [redacted].

Interview of [redacted]

[redacted] told the OI [redacted] was not pressured or instructed to subcontract with [redacted]. Because [redacted] was not familiar with the specific skills needed to perform the assessment, he solicited recommendations from [redacted] contractors and NARA employees. During a conversation about possible vendors [redacted] told [redacted] that [redacted] did excellent work for [redacted] while [redacted] was employed there. [redacted] heard that NARA was very pleased with [redacted] work on the assessment [redacted] subcontracted with [redacted] without competition.

OI Review of Documentation from [redacted], BCN

[redacted] provided the OI the following documents missing from the contract files for [redacted] and [redacted] during the OI review:

- [redacted] to extend the contract for 6 months.
- Five invoices for [redacted] billed NARA $16,122.26 for 105.25 hours of subcontracted work performed by [redacted] on the assessment.
- Two invoices [redacted] billed NARA $4,987.13 for 32.5 hours of subcontracted work performed by [redacted] on the assessment.

OI Interview of [redacted]

In early 2012, one of the Contracting Officer's Technical Representatives (COTR), who [redacted] could not name, told [redacted] that NARA needed [redacted] assessment [redacted] for OPA. [redacted] told [redacted] and [redacted] that [redacted] could perform the assessment under their management and operating contract. However, [redacted] stated [redacted] got the impression they did not think [redacted] was capable of performing the assessment and wanted to use an outside contractor.

[redacted] told [redacted], [redacted] was concerned about [redacted] and [redacted] looking for an outside contractor, but never received a response from [redacted]. Later, [redacted] Office of Acquisitions, removed [redacted] as [redacted] and replaced [redacted] with [redacted]. [redacted] believes [redacted] removed [redacted] from the contract because of complaints from [redacted] and [redacted]

The OI showed [redacted] both [redacted] and [redacted]. Based on [redacted] review of the contract documentation [redacted] did not believe there was any violation of the Federal Acquisition Regulations or

REPORT OF INVESTIGATION (Continued)

NARA contracting regulations. [redacted] told the OI that [redacted] could perform the work under the [redacted], but [redacted] expected there would be a TDL or task order which directed the assessment, although it was not required.

OFFICE OF INSPECTOR GENERAL

OFFICE OF INVESTIGATIONS

REPORT OF INVESTIGATION:

14-0006-I

WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
14-0006-I	Documents Concealed in Researcher's Clothing	
Period of Investigation: December 12, 2013	**Type of Report:** ☐ Interim ☒ Final ☐ Supplemental	**Distribution:** ☒ Info Only ☐ Referred ☐ Closed to File

SUBJECT(S) OF INVESTIGATION

[redacted]

BASIS FOR INVESTIGATION

On December 12, 2013, [redacted] Holdings Protection Team (HPT), Security Management Division (BX), National Archives and Records Administration (NARA), and [redacted] HPT, reported to the OI that on December 9, 2013, [redacted], NARA contractor, saw an unidentified researcher with documents concealed under [redacted] clothing in an Archives II restroom adjacent to the Research Rooms. [redacted], National Archives Trust Fund Branch, was with [redacted] but did not see the documents.

ALLEGED VIOLATIONS

18 USC § 641: [Theft of] Public money, property or records

18 USC § 2071: Concealment, removal, or mutilation generally [of Federal records]

NARA Policies and Directives

RESULTS OF INVESTIGATION

The OI identified and interviewed the researcher, [redacted], at Archives II. [redacted] admitted [redacted] concealed documents in [redacted] clothing and left Archives II with those documents. [redacted] denied the documents were NARA holdings and claimed they were [redacted] personal papers. The OI conducted consensual searches of [redacted] researcher locker, vehicle, and apartment and found no evidence [redacted] stole NARA holdings.

Prepared by: [redacted]	Signature: [redacted]	Date of Report: February 18, 2014
Approved by: AIGI Matthew Elliott	Signature:	

REPORT OF INVESTIGATION (Continued)

INVESTIGATIVE SUMMARY

Initial Report to HPT

On December 9, 2013, [redacted] and [redacted] notified student employee, [redacted], Archival Operations-Washington, DC (RD-DC) about the suspicious [redacted] researcher. The same day, [redacted] reported the incident to another student employee, [redacted] RD-DC who then informed [redacted], RD-DC. On the morning of December 11, 2013,[1] [redacted] reported the incident to [redacted] and [redacted].

OI Interviews of [redacted] and [redacted]

[redacted] and [redacted] stated the incident occurred in the 4th floor [redacted] restroom adjacent to the 4th floor Research Room. [redacted] said [redacted] and [redacted] were in separate bathroom stalls when [redacted] entered the bathroom. [redacted] stood facing [redacted] stall and lifted [redacted] clothing. When [redacted] did, [redacted] saw papers stuffed under [redacted] outer garments. [redacted] appeared to notice [redacted] and [redacted] inside the stalls and quickly left the bathroom. [redacted] described the unidentified [redacted] wearing a grey [redacted] sweater.

[redacted] and [redacted] left the [redacted] restroom to look for [redacted] in the immediate area. They did not see [redacted] so they then went to the 4th floor Research Room and reported the incident to a NARA employee.[2] They also unsuccessfully attempted to locate [redacted] in the 4th floor Research Room and two additional research rooms.

OI Review of Archives II Security Camera Video Footage

Video footage during the time of the incident from cameras adjacent to the 4th floor Research Room shows both [redacted] and [redacted] walk towards the restrooms located next to the Research Room. Approximately two minutes later, the same video shows [redacted] wearing grey clothing leaving the 4th floor Research Room and walk towards the same restrooms. A short time later [redacted] and [redacted] can be seen entering the 4th floor Research Room and stopping at the employee desk. [redacted] and [redacted] then continue into the Research Room, and appear to be searching for [redacted].

Video footage on December 9, 2013 also shows the same [redacted] researcher leaving the Archives II research area through the 1st floor Research Room security checkpoint at about 1:26 p.m.

[1] On December 10, 2013, Archives II was closed due to inclement weather. On December 11, 2013 [redacted] and [redacted] were both on annual leave, so they didn't receive the voicemail from [redacted] until December 12, 2013.
[2] The employee was later identified as [redacted].

Investigation Number:	Case Title:
14-0006-I	Documents Concealed in Researcher's Clothing

REPORT OF INVESTIGATION (Continued)

OI Identification and Interview of [redacted]

OI Identification of [redacted] using the Archives II Researcher Database

[redacted] RD-DC, queried the Archives II researcher database and determined someone using researcher card [redacted] left the 1st floor researcher checkpoint at approximately 1:26 p.m. on December 9, 2013. [redacted] further determined researcher card [redacted] is assigned to [redacted]. The photograph associated with [redacted] in the Archives II researcher database met the description [redacted] and [redacted] provided.

OI Interview of [redacted]

On December 12, 2013, the OI located [redacted] matching [redacted] description in the Archives II 2nd floor Research Room and confirmed [redacted] was assigned researcher card number [redacted] [redacted] spoke only limited English and [redacted] co-worker, [redacted] assisted in translating. The OI explained to [redacted] the allegations [redacted] and [redacted] had made against [redacted]. [redacted] then admitted [redacted] concealed documents in [redacted] clothing on December 9, 2013. However, [redacted] explained the documents were personal insurance documents, not NARA holdings. [redacted] stated [redacted] forgot to have [redacted] personal documents stamped by security when [redacted] arrived at Archives II earlier in the day. [redacted] further explained [redacted] wanted to give the documents to a fellow researcher to make copies. Finally, [redacted] said [redacted] was embarrassed, so [redacted] hid the documents rather than admit [redacted] mistake to NARA security.[3]

OI Consent Searches of [redacted] Property

The OI conducted consensual searches of [redacted] NARA researcher locker, vehicle and apartment and found no evidence [redacted] stole NARA holdings.

[3] NARA requires all researchers complete an orientation before being issued a researcher card. The orientation indicates, in part, that Research Room staff must inspect and approve any documents researchers wish to bring into the Research Room.

Investigation Number:	Case Title:
14-0006-I	Documents Concealed in Researcher's Clothing

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
14-0010-I	Computer Misuse - [redacted]	
Period of Investigation:	**Type of Report:**	**Distribution:**
February 2014 - May 2014	☐ Interim ☒ Final ☐ Supplemental	☐ Info Only ☒ Referred ☐ Closed to File

SUBJECT(S) OF INVESTIGATION

[redacted]
National Archives and Records Administration (NARA)

BASIS FOR INVESTIGATION

On January 30, 2014, based on information received from the NARA Inappropriate Use Working Group (IUWG), the NARA, Office of Inspector General, Office of Investigations, Computer Crimes Unit (CCU), initiated an investigation and independently identified that between January 28 and 29, 2014, [redacted] attempted to access blocked websites with sexually suggestive titles.

ALLEGED VIOLATIONS

18 U.S.C. §1030 - Fraud and Related Activity in Connection with Computers

NARA Policies and Directives

RESULTS OF INVESTIGATION

This investigation substantiated that, for at least the past 5 years [redacted] used [redacted] NARA computer and other NARA IT assets to access pornographic material on the internet, store pornographic images, and engage in personal activities related to [redacted] interest in nudity and pornography. The CCU interviewed [redacted] who admitted [redacted] knowingly misused NARA IT assets in violation of NARA Policies and Directives.

Prepared by:	Signature:	Date of Report:
[redacted]	[redacted]	June 13, 2014
Approved by: IG(A) James Springs	**Signature:**	

REPORT OF INVESTIGATION (Continued)

INVESTIGATIVE SUMMARY

Referral from the IUWG

Over several months, the IUWG identified high levels of prohibited activity on [redacted] user profile. A review of the blocked activity by the IUWG members identified the activity as pornographic in nature, so they referred the matter to the CCU.

A review of the information provided by the IUWG identified the blocked activity appeared to directly relate to pornographic websites.

Review of [redacted] Network Storage Drive[1]

A review of the material stored on [redacted] network drive identified thousands of images of partially clothed or nude women engaging in sexual activity. The review also identified several images of [redacted] standing nude in what was later determined to be the now defunct [redacted]. In the pictures, [redacted] is depicted nude in front of a piece of art with a large downward arrow painted on [redacted] torso with the words, "Warning Choking Hazard" painted above and below the arrow.

Results of Computer Forensic Examination

In February 2014, the CCU made a forensic image of the hard drive from [redacted] NARA computer and conducted a forensic examination on the drive's contents. The examination identified several thousand images of pornography downloaded from the Internet and saved to [redacted] network storage drive. The images depicted nude women engaging in sexual acts. The images were in the recovered Temporary Internet Files folder and in thumbnail image files throughout the [redacted] user profile. *(Exhibit 1)*

OI Interview of [redacted]

On April 24, 2014, the CCU interviewed [redacted], with [redacted] attorney present, and [redacted] admitted to using [redacted] NARA computer to search out and store pornographic images during and after work hours. [redacted] also admitted to using [redacted] Government computer and email to engage in personal activities related to [redacted] and [redacted] interest in nudist resorts in the area.

During the interview [redacted] stated that for more than 5 years [redacted] has used [redacted] NARA computer to look for, download, and save pornographic images - activity [redacted] knew violated NARA Directive 802. [redacted] stated [redacted] preferred to use [redacted] NARA email address to engage in personal communication because [redacted] could see responses faster. *(Exhibit 2)*

[1] Each NARA computer user has a network storage drive where they can upload files and access them from almost any NARA networked computer.

OFFICE OF INSPECTOR GENERAL

OFFICE OF INVESTIGATIONS

REPORT OF INVESTIGATION:

14-0013-I

WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
14-0013-I	Time and Attendance Fraud / Transit Program Benefit Fraud – Civilian Personnel Records Center	
Period of Investigation: April 2014 – July 2014	**Type of Report:** ☐ Interim ☒ Final ☐ Supplemental	**Distribution:** ☐ Info Only ☐ Referred ☒ Closed to File

SUBJECT(S) OF INVESTIGATION

Employee X[1]

BASIS FOR INVESTIGATION

On April 1, 2014, [redacted], National Personnel Record Center (NPRC) reported to the Office of Inspector General (OIG) - Office of Investigations (OI) allegations that Employee X, Archives Technician, Civilian Personnel Records (AFN-CO), was signing [redacted] time cards to reflect an arrival time earlier than [redacted] actual arrival time. It was alleged Employee X was receiving Public Transit Subsidy Program (Transit Program) benefits while driving to work at the Civilian Personnel Records Center (AFN-CO) in Valymeyer, IL.

ALLEGED VIOLATIONS

18 USC 641: Public money, property or records

18 USC 1001: Statements or entries generally

NARA Policy and Procedures

RESULTS OF INVESTIGATION

[1] The NARA employee will not be identified as a subject in this report as the NARA OIG did not conduct an interview of the subject.

Prepared by:	Signature:	Date of Report:
SA [redacted]	[redacted]	September 8, 2014
Approved by: Acting AIGI James Springs	James Springs	

REPORT OF INVESTIGATION (Continued)

Alleged Transit Program Fraud

The OI determined Employee X is authorized to drive a personal vehicle from time-to-time to work while simultaneously receiving the Transit Program benefit. The OI determined Metro Transit-St. Louis does not provide direct service to the Valmeyer facility, resulting in employees carpooling to Valmeyer for a portion of their commute. This lack of direct service may create the appearance employees are improperly driving to work – when, instead, they may use public transportation to meet off-site before carpooling the remaining distance to Valymeyer.

Employee X's supervisors authorized [redacted] to receive the Transit Program benefit in 2012 and 2013 without requiring Employee X to describe [redacted] intended public transportation route to and from work. NARA has no policy requiring employees to completely describe their intended home-to-work commuting route via public transportation. Lack of route information presents hurdles to the Government's ability to maintain oversight and to investigate suspected instances of fraud relating to Transit Program benefits.

Alleged Time Card Fraud

The AFN-CO could only provide Cardholder Reports[2] dating back six months. The OI compared Employee X's time cards against the corresponding Cardholder Report for September 16, 2013 through March 13, 2014, which revealed the following:

- On 48 occasions, Employee X's time cards indicated an arrival time earlier than the Cardholder Report for [redacted] badge, a potential loss to the Government.
- On 25 occasions, Employee X's time cards indicated an arrival time later than the Cardholder Report for [redacted] badge, a potential gain to the Government.
- The OI found that the potential lost time to the Government could be approximated as 11.53 employee work hours (approximately $192.55).[3]

Coordination with U.S. Attorney's Office

On June 9, 2014, The United States Attorney's Office (USAO) for the Southern District of Illinois declined to prosecute the suspected time and attendance fraud and the suspected Transit Program benefit fraud.

[2] These reports reflect the use of Employee X's badge at [redacted] located at AFN-CO.
[3] Employee X's hourly salary is $16.70.

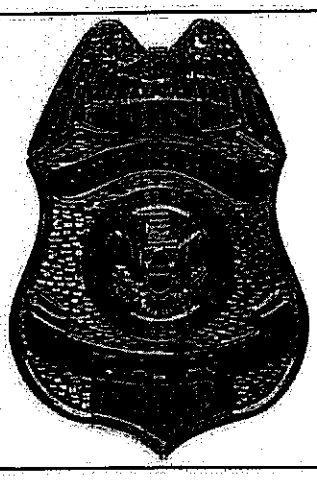
Investigation Number:	Case Title:
14-0013-I	Time and Attendance Fraud / Transit Program Benefit Fraud – Civilian Personnel Records Center

REPORT OF INVESTIGATION (Continued)

OI Interview of Employee X

The OI determined it would not be within the best interest of the Federal Government to incur travel costs to interview the subject based on the following: 1) the USAO declined prosecution, 2) AFN-CO could only provide six months of documentation concerning Employee X, 3) Employee X's supervisors interviewed [redacted] prior to notifying to the OI, 4) the potential loss was approximately $192.55, and 5) Employee X's supervisors are coordinating with the Office of Human Capital (H) for potential discipline.

Investigation Number:	Case Title:
14-0013-I	Time and Attendance Fraud / Transit Program Benefit Fraud – Civilian Personnel Records Center



OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

REPORT OF INVESTIGATIONS

Case Number: 14-0014-I

WARNING

The attached document may contain information protected by Federal confidentiality statues prohibiting unauthorized access and disclosure of its contents to any person other than the intended recipient(s) or those with an official need for access. The contents of this document should not be left unattended.

REPORT OF INVESTIGATION

Investigation Number:	Case Title:	
14-0014-I	President Andrew Jackson Pardon of Zachariah Smith	
Period of Investigation: March 2013-October 2014	**Type of Report:** ☐ Interim ☒ Final ☐ Supplemental	**Distribution:** ☐ Info Only ☐ Referred ☒ Closed to File

SUBJECT(S) OF INVESTIGATION

N/A

BASIS FOR INVESTIGATION

On March 19, 2013, [redacted] National Archives and Records Administration (NARA), reported to the Office of the Inspector General (OIG), Office of Investigations (OI), Archival Recovery Team (ART) initial findings of an internet search [redacted] conducted for missing NARA records. During [redacted] search, [redacted] found a 2004 sale through [redacted] which listed a presidential pardon matching the description of a pardon listed on NARA's Missing Documents website. The document was a President Andrew Jackson pardon of Zachariah Smith, dated July 5, 1835.

ALLEGED VIOLATIONS

18 U.S.C. § 668: Theft of Major Artwork
18 U.S.C. § 2071: Concealment, Removal, or Mutilation Generally

RESULTS OF INVESTIGATION

This investigation was unable to identify the person(s) responsible for the removal and theft of the historical record from NARA's holdings. The OI was unable to recover the missing pardon.

The OI issued an administrative subpoena to [redacted] to collect records involving the auction of the Andrew Jackson pardon. The OI review of the subpoena documentation found that [redacted] located in Aspen, Colorado offered the pardon for sale through the online auction. [redacted] from [redacted] was listed as the winner for the auction involving the pardon.

The OI determined that [redacted] was no longer in business and tracked the former owner, [redacted] to a real estate development company in [redacted]. The OI interviewed [redacted] who confirmed that [redacted] went out of business in 2004. [redacted] maintained all business and tax records in a

Prepared by:	Signa[redacted]	Date of Report:
Special Agent[redacted]		27OCT2014
Approved by:	Signa[redacted]	

REPORT OF INVESTIGATION (Continued)

storage facility until 2010 at which time they were destroyed. [redacted] was unable to recall the sale of the document since [redacted] purchased and sold hundreds of presidential documents. [redacted] told the OI that [redacted] was not the legitimate purchaser of the document as listed on the sales paperwork. [redacted] explained that [redacted] would use [redacted] online buyer profile to increase the bids on historical documents [redacted] posted for sale on auction websites, to include [redacted].

The OI interviewed [redacted] and confirmed that [redacted] gave [redacted] user name and password and authorized [redacted] to bid on auction items listed online. However, [redacted] was not involved with the auction and did not monitor [redacted] use of [redacted] account [redacted] is a close friend of [redacted] and is not a historical document collector. [redacted] was unable to provide the OI with any bidding records from [redacted] buyer profile.

This investigation was not presented to the Department of Justice (DOJ) for prosecution based on insufficient evidence.