



OFFICE OF INSPECTOR GENERAL

JULY 25, 2022

Evaluation of the Architect of the Capitol's Security Badging Program

Evaluation Report 2022-0001-IE-P

MISSION

The OIG promotes efficiency and effectiveness to deter and prevent fraud, waste and mismanagement in AOC operations and programs. Through value added, transparent and independent audits, evaluations and investigations, we strive to positively affect the AOC and benefit the taxpayer while keeping the AOC and Congress fully informed.

VISION

The OIG is a high-performing team, promoting positive change and striving for continuous improvement in AOC management and operations. We foster an environment that inspires AOC workforce trust and confidence in our work.



Results in Brief

Evaluation of the Architect of the Capitol's Security Badging Program

July 25, 2022

Objective

Our objective for this evaluation was to assess the security badging process for the Architect of the Capitol (AOC) employees and contractors to determine if vulnerabilities exist within the program. This evaluation was consistent with our 2021 agency Management Challenges that listed Balancing Safety and Security with Preservation and Heritage as a Management Opportunity and Performance Challenge. At the AOC, the Office of the Chief Security Officer (OCSO) is assigned responsibility for the security badging program.

Findings

Based on our evaluation, we found the following:

- The AOC lacked a standardized badging policy for AOC employees, and the existing suitability policy for contractors is outdated and lacked timely revision.
- The AOC badging process was inefficient, with process gaps and a system of record that was outdated and inadequate.
- The AOC security badging program lacked adequate security processes for protection of Personally Identifiable Information (PII) and physical badges.
- Inadequate badging information sharing between the AOC, the House of Representatives Sergeant at Arms (HSAA) and the United States Capitol Police (USCP), with reliance on outdated means of communication, with the potentiality of

security gaps in notification as well as duplication of effort.

Recommendations

We recommend that:

1. The Office of the Chief Security Officer develop and implement a suitability policy for AOC employees and consolidate and implement revisions, as appropriate, to the current contractor suitability policy. Additionally, develop and implement a standardized timeline for policy revision and update within the current Fiscal Year.
2. The Office of the Chief Security Officer, in coordination with the USCP and the HSAA, perform a joint feasibility study to consider:
 - Re-assigning signature authority for the CP-491 for HSAA-issued contractor badges from the OCSO to Contracting Officer Representatives, eliminating the hand carry of the CP-491 to USCP/Fairchild for Fingerprinting, and implementing the use of approval buttons or pdf secure signatures in place of manual signatures.
 - Identification, development or acquisition of a badge management software solution that uses notification-based processes that ensures secure, efficient execution, monitoring and tracking of badging actions.
3. The Office of the Chief Security Officer develop and implement suitability policy language to include clear lines of responsibility and processes. Improvements should include:
 - In the contractor suitability policy, assign the responsibility for the centralized recordkeeping of intra-agency badging agreement Memorandums of Understanding



Results in Brief

Evaluation of the Architect of the Capitol's Security Badging Program

- or Agreements to the Office of the Chief Security Officer; and
 - In both policies, guidance and requirements for secure badge return and protection and oversight of PII.
4. The Office of the Chief Security Officer in coordination with the USCP and the HSAA, perform a joint feasibility study to develop and implement a centralized security badge management process through the use of shared software that allows for secure and efficient issuance, monitoring and tracking of badging actions, to include tracking and reporting of lost/stolen badges and follow-up actions.

Management Comments

The AOC provided comments on July 12, 2022, see Appendix B. In its Management Comments, the AOC concurred with two findings and recommendations. The AOC either concurred, non-concurred or partially concurred with the other two recommendations. Please see the recommendations table on the next page for the status of the recommendations.



Results in Brief

Evaluation of the Architect of the Capitol's Security Badging Program

Recommendations Table

Responsible Entity	Recommendation Resolved	Recommendation Unresolved	Recommendations Closed
OSCO	R1, R3	R2, R4	

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** - Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** - Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – The Office of Inspector General verified that the agreed upon corrective actions were implemented.



INSPECTOR GENERAL

DATE: July 25, 2022

TO: J. Brett Blanton
Architect of the Capitol

FROM: Christopher P. Failla, CIG
Inspector General

SUBJECT: Evaluation of the Architect of the Capitol's (AOC's) Security
Badging Program (Project No. 2022-0001-IE-P)

Please see the attached final report for our evaluation of the AOC's Security Badging Program, which was announced on November 10, 2021. We found that at the AOC's security badging program was inefficient and had significant security vulnerabilities. This report includes four recommendations for improvement to the AOC's security badging program.

In your response to our official draft report (Appendix B), you concurred with two recommendations and provided neither concurrence nor non-concurrence with two recommendations. Based on your response to Recommendations 1 and 3, we feel the proposed corrective actions address our recommendations. However, your proposed concurrence, non-concurrence or partial concurrence with Recommendations 2 and 4 do not adequately address our expressed need for improvements to this program's efficiency and security as discussed in our report. The status of the recommendations will remain open until final corrective action is taken. We will contact you within 90 days to follow-up on the progress of your proposed management decision.

I appreciate the assistance you and your staff provided throughout the evaluation. Please direct questions to Evaluator Audrey Cree at 202.631.2682, or Audrey.Cree@aoc.gov or Assistant Inspector General for Inspections and Evaluations Chico Bennett at 202.394.2391, or Chico.Bennett@aoc.gov.

Distribution List:

Valerie Hasberry, Chief Security Officer
Jason Baltimore, General Counsel
Peter Bahm, Chief of Staff
Mary Jean Pajak, Deputy Chief of Staff

Contents

INTRODUCTION	1
OBJECTIVE	1
BACKGROUND.....	1
REVIEW OF INTERNAL CONTROLS	2
CRITERIA	3
FINDING 1	3
STANDARDIZED SUITABILITY POLICY FOR AOC EMPLOYEES AND CONTRACTORS	3
CONCLUSION.....	5
RECOMMENDATION	5
FINDING 2	6
INEFFICIENT AND INADEQUATE BADGING PROCESS.....	6
CONCLUSION.....	11
RECOMMENDATION	11
FINDING 3	1
AOC BADGE SECURITY AND PROTECTION OF PII	1
CONCLUSION.....	3
RECOMMENDATION	3
FINDING 4	4
INTERAGENCY SECURITY BADGING COMMUNICATION PROCESSES WERE OUTDATED AND INADEQUATE4	
CONCLUSION.....	7
RECOMMENDATION	7
OBSERVATIONS.....	8
APPENDIX A.....	11
SCOPE AND METHODOLOGY	11
USE OF COMPUTER-PROCESSED DATA.....	11
PRIOR COVERAGE	11
APPENDIX B.....	12
MANAGEMENT COMMENTS	12
ANNOUNCEMENT MEMO	15
ACRONYMS AND ABBREVIATIONS.....	16

Introduction

Objective

The objective of this evaluation was to assess the security badging process for the AOC employees and contractors to determine if vulnerabilities exist within the program.

Background

Congressional identification (ID) (security badges) issuing authorities are the U.S. House of Representatives (tasked to the House Sergeant at Arms (HSAA)), the U.S. Capitol Police (USCP), the U.S. Senate (tasked to the Senate Sergeant at Arms (SSAA)), the Library of Congress and the Supreme Court. Congressional ID policy is governed by an Identification (ID) Standardization Task Force,¹ established by the Capitol Police Board² in 2006, and lead by the USCP's Security Services Bureau. In coordination with the U.S. House of Representatives and U.S. Senate, the task force developed a Congressional Identification Policy Manual and a Change Management Board consisting of a management representative from each Capitol Police Board entity. This group is tasked with vetting proposed changes to the manual prior to submittal to the Capitol Police Board. Additionally, the Change Management Board is also tasked with reviewing and updating the manual and templates at least six months before the end of a Congressional session.

Security badges for AOC employees, contractors and visitors are issued by the HSAA, working in conjunction with the USCP and the AOC's Office of the Chief Security Officer³ (OCSO), the AOC's lead authority for the program. The USCP also oversees and implements a separate security badging process for project site-specific AOC contractor badges (called Unified Construction IDs (UCIDs) or Project Specific IDs), and site-specific badging for AOC contractors at the Capitol Power Plant. Project specific IDs are issued based on a Memorandum of Understanding (MOU) between the OCSO and the USCP. Security badges for AOC employees and

¹ This group was tasked to increase security, reduce fraud and system abuse, increase efficiency and effectiveness, and achieve uniformity of ID processes and practices by standardizing the Congressional ID system campus-wide.

² Capitol Police board entities consist of the U.S. Senate Sergeant at Arms and Doorkeeper, the U.S. House of Representatives Sergeant at Arms, the Architect of the Capitol, and the USCP Chief of Police (who serves in an ex-officio, non-voting capacity) (retrieved February 24, 2022 from <https://www.uscp.gov/the-department/oversight/capitol-police-board>)

³ In 2020, the Architect of the Capitol announced an organizational transformation initiative, which included a change in reporting structure to address confusing chains of accountability and authority. As a result, while the April 13, 2017 supplement to Order 731-1 references the Office of Security Programs as the office of professional responsibility for suitability processes, that department was re-named in 2020 as the Office of the Chief Security Officer. Retrieved October 22, 2021 from <https://www.compass.aoc.gov/office-of-the-architect/organizational-transformation/big-rocks-agency-initiatives/reorganization>

contractors working in Senate Office Buildings are also issued by the HSAA, as are those working in the Library of Congress and the Supreme Court. The latter also requires that all contractors are escorted at all times.

Security badge access rights are controlled by the USCP for all badging entities, with the exception of the Supreme Court, in accordance with USCP Directive 1040.004;⁴ designation of access permission levels for AOC employees is provided by AOC officials per this Directive.

During the period of review, the AOC did not have an agency-specific policy for the issuance, use, security and return of AOC employee security badges, although it did for suitability screening and security badge management processes for contractors.⁵ The AOC is in the process of revising its contractor suitability policy, and issuing a new suitability policy for AOC employees; these policies include the assignment of responsibilities for badging processes. An AOC “Compass” intranet site has a badge portal that provides guidance for security badging processes, documentation requirements and training. Guidance further describes the portal as a secure database for storing and protecting Personally Identifiable Information (PII) and as a place to view badge request status. This guidance also describes the portal as a location from which users can run reports for auditing but does not offer significant information about this reporting capability or who might use it. At the time of this report, there were approximately 3,700 House ID-issued badges in use by AOC staff, and approximately 1,760 USCP project site-specific badges for AOC contractors. In the prior year, there were approximately 7,000 to 8,000 AOC badges issued by the HSAA.

Review of Internal Controls

We evaluated the AOC’s internal controls for its security badging program. Although the AOC had an agency-wide policy governing contractor suitability, which addressed badging processes, there are deficiencies that exist with the current security badging program activities, and there was no companion policy for AOC employees. As a result, the lack of updated internal controls and associated policies creates the potential for process gaps and vulnerabilities within the AOC security badging framework.

⁴ USCP Directive 1040.004, Access Control Clearance Management, covers the granting and management of the electronic clearance code access lists via the USCP Access Control System. This Directive establishes transparent, repeatable, and auditable processes to ensure that access to security areas is only provided to authorized personnel.

⁵ Order 731-1, Contract Employee Suitability, January 9, 2012 with supplements issued April 15, 2015; April 13, 2017; and January 26, 2018. The April 13, 2017 supplement included a change in assignment of office of professional responsibility for the suitability process from administration by the Human Capital Management Division to the Office of Security Programs.

Criteria

The following criteria were used during this evaluation:

- AOC Order 296-4 Off-Boarding Separating Employees
- AOC Compass Intranet Badge Tracking Portal Guidance Documents:
 - Badge Tracking Portal Training Video 4.27.21
 - OCSO Badge Portal FAQs 6.24.21
 - OCSO Badge Portal Guide 6.24.21
 - OCSO Badge Portal Requests 6.24.21
 - Out-of-State Fingerprint Instructions
- Order 34-1 AOC Contracting Manual (2020)
- Order 731-1 Contractor Suitability Policy with Supplements

Finding 1

Standardized Suitability Policy for AOC Employees and Contractors

We found that the AOC lacked a standardized badging policy for AOC employees, and the existing suitability policy for contractors is outdated and lacked timely revision.

This occurred because:

- The AOC had no existing policy for AOC employee suitability; communication of processes and standards for AOC employee badging instead relied on numerous training venues, while guidance documents and Standard Operating Procedures (SOPs) lacked the authority of formal policy;
- The AOC contractor suitability policy process and supplements were not consolidated into one comprehensive policy;
- Supplements to the suitability policy addressed changes to the program over time, to include transfer of oversight responsibilities from the Chief Administrative Officer (CAO) to the OCSO; and
- The AOC efforts to develop new and revised suitability policy lacked timeliness and consistency of effort.

As a result, the lack of standardized and updated policies and procedures increased the probability of security vulnerabilities and gaps in the AOC security badging process. In addition, the lack of timeliness for the policy update increased the risk to program cohesiveness.

Discussion

The AOC is responsible for the maintenance, operation, development and preservation of 18.4 million square feet of buildings and more than 570 acres of land throughout the Capitol complex. There is a shared responsibility amongst the AOC, HSAA and USCP to ensure that AOC employees and contractors have the proper security badging access to buildings and facilities across the Capitol complex. Security badging practices are governed under 2 USC §4101 and 2 USC §1831, and the HSAA and USCP have separate badging policies and directives. However, during our review, we found the AOC lacked a standardized badging policy for AOC employees, and the existing policy for contractors is outdated and lacked timely revision.

The AOC had no existing policy for AOC employee suitability; communication of processes and standards for AOC employee badging instead relied on numerous training venues, while guidance documents and SOPs lacked the authority of formal policy. Guidance and requirements for recordkeeping and protection and oversight of PII was inadequate, and responsibilities for centralized agency recordkeeping of intra-agency badging MOU or Memorandums of Agreement (MOAs) were not addressed. AOC employee badging guidance was not consolidated into one comprehensive policy, and changes to the program over time, to include transfer of oversight responsibilities from the CAO to the OCSO, were not reflected in other AOC policies or guidance related to badging.⁶ Although the AOC lacked policy governing determinations of suitability and the issuance, control and return of identification badges for AOC employees, there was a policy for AOC contractor personnel. The contractor policy included numerous supplements that needed consolidation to ensure clarity. The lack of formal policy resulted in gaps in recordkeeping as well as uneven processes across jurisdictions for badge return and safeguarding of PII.

The AOC efforts to develop new and revised suitability policy lacked timeliness and consistency of effort. At the time of our review, the AOC had been in the process of developing a suitability policy for its employees for a few years, but these efforts did not result in issued policy. AOC badging officials attributed delays in policy development to ongoing conversations within the Legislative Branch about changes to the AOC's suitability standards and their impact on other Legislative Branch agencies. The AOC's concerns centered on implementing suitability standards, such as Tier 1⁷ background investigations and regular reviews per position, that ensure that

⁶ Both AOC Order 296-4, Off-Boarding Separating Employees, February 12, 2015, and AOC Contracting Officer Representative (COR) appointment letters continue to reference the CAO's Human Capital Management Division as a lead authority or point of contact for badging processes.

⁷ Tier 1 is the investigation for positions designated as low-risk, non-sensitive. It is also the minimum level of investigation for a final credentialing determination for physical and logical access. Tier 1 investigations are requested using standard form (SF) 85. Retrieved March 31, 2022 from <https://www.dcsa.mil/Portals/91/Documents/pv/GovHRSec/FINs/FY15/fin-15-03.pdf>

AOC employees would not be a cause of damage or threat within the Capitol complex. The OCSO is currently engaged in efforts to develop official SOPs or policy memoranda to document interaction with UCSP events, as well as formal MOAs and MOUs for agreements reached with the USCP. AOC badging officials also noted that policy development was impacted by the security incidents of January 6, 2021, and further discussion of how the Legislative Branch should, as a whole, address suitability and background checks.

Impact

As a result, the lack of standardized and updated policies and procedures increased the probability of security vulnerabilities and gaps in the AOC security badging process. In addition, the lack of timeliness for the policy update increases the risk to program cohesiveness and allows for uneven implementation of security processes. Lack of formal security badging policy has resulted in badge issuance, recordkeeping and retrieval guidance that is largely provided via training and documents on the AOC's badge portal. In addition, non-standardized procedures have resulted in the OCSO not having visibility into all Agency/USCP MOUs/MOAs pertaining to security badging.

Conclusion

Standardizing and updating AOC security badging policies and procedures can help AOC organizations reduce potential security vulnerabilities. While there are numerous guidance documents and trainings on portal use, these are largely related to process issues and lack the authority and assignment of responsibilities of formal policy. The Office of Inspector General (OIG) efforts to obtain copies of MOUs/MOAs with USCP and within the AOC were met with limited success, revealing a lack of centralized authority and knowledge of Capitol complex access issues. Timely review, update and implementation of standardized policies and procedures can improve security badging program cohesiveness and minimize process gaps.

Recommendation

Recommendation 1

We recommend the Office of the Chief Security Officer develop and implement a suitability policy for AOC employees and consolidate and implement revisions, as appropriate, to the current contractor suitability policy. Additionally, develop and implement a standardized timeline for policy revision and update within the current Fiscal Year.

AOC Comment

The AOC concurs. The Office of the Chief Security Officer (OCSO) staff have completed coordination of the draft AOC Order 42-6, Staff Personnel Suitability

Program Policy, with the Human Capital Management Division and are finalizing the associated forms. The draft order will enter the AOC's publication process no later than July 15, 2022. The OCSO has also drafted AOC Order 42-7, Contractor Suitability Policy, which will replace Order 731-1, Contractor Suitability Policy. The draft of AOC Order 42-7 will be entered into the AOC's publication process no later than September 1, 2022, after resolution of outstanding comments. The OCSO will conduct annual reviews of both orders no later than March 31st of each year.

OIG Response

We reviewed the management comment and determined it addresses the finding and recommendation.

Finding 2

Inefficient and Inadequate Badging Process

We found that the AOC badging process was inefficient, with process gaps and a system of record that was outdated and inadequate.

This occurred because:

- The AOC security badging utilizes a manpower- and paperwork-intensive process that requires close interaction and information sharing between AOC and its contractor personnel, and with the HSAA and USCP;
- The AOC badging process requires the submission of four individual forms (an HSAA Congressional ID Request form, a USCP CP-491, an E-Verify verification document, and a photo of the applicant's valid (non-expired) government photo identification) to a SharePoint intranet site accessible only to AOC employees; and
- Processes for form submittal are cumbersome, duplicative and inadequate; minimal automation and gaps in notification systems allow for insecure and inefficient execution, monitoring and tracking of badging actions.

As a result, the lack of an efficient and adequate badging process increased the probability for security vulnerabilities, acts of criminality and process gaps within the AOC badging program.

Discussion

AOC processes for badge issuance are conducted via AOC's "Compass" intranet web site, which includes a badge request portal on its home page. Training and guidance

are included within the portal, and its purpose is described as serving as “a centralized portal to submit and retain required documentation for the suitability and ID process.” During our review, we found that the AOC badging process was inefficient, with process gaps and a system of record that was outdated and inadequate.

Badge Request Processes

The AOC security badging portal utilizes a manpower- and paperwork-intensive process that requires close interaction and information sharing between AOC and its contractor personnel, and with the HSAA and the USCP. The AOC’s Office of the Chief Engineer (OCE) noted that it is additionally challenged by having to engage in two separate processes for contractor badging; one for AOC Contractor Badges processed through the OCSO and HSAA system (which is better defined and has some automated processes for actions and notifications, such as approvals for badge pick-up), and a separate process for larger contracts that require “Project Specific Badges” (UCIDs) which are issued by the USCP. Although the OCE noted that the USCP UCID process has minimal automation and badges are renewed annually; they found badge management on these projects to be labor intensive, with management of paperwork more difficult.

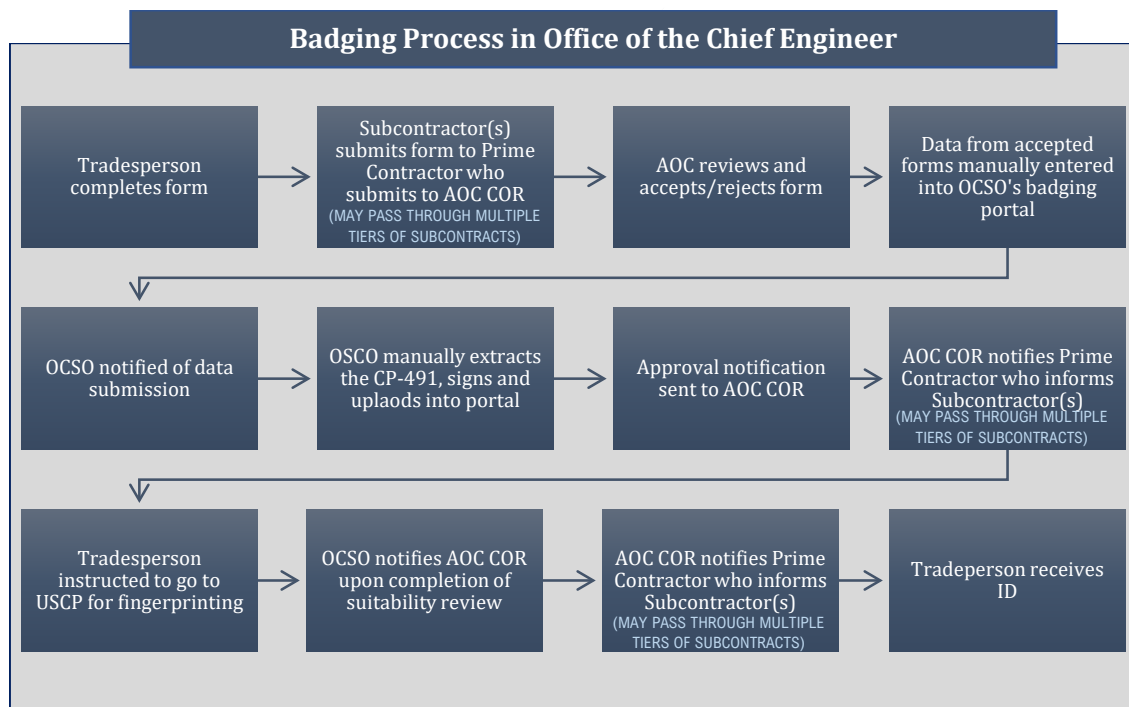


Figure 1: HSAA Badging form process as experienced by OCE CORs

Figure 1 above indicates the HSAA badging form submittal, review and approval process as experienced by OCE CORs, and highlights process insecurities. The HSAA/AOC badging process requires the submission of four applicant forms (an

HSAA Congressional ID Request, a USCP CP-491 request for check of criminal history, an E-Verify verification document, and a photo of the applicant's valid (non-expired) government photo identification), containing significant amounts of PII to a SharePoint intranet site accessible only to AOC employees. Our review of the badging process indicated that processes for form submittal are cumbersome, duplicative and inadequate. Minimal automation and gaps in notification systems allow for insecure and inefficient execution, monitoring and tracking of badging actions. To submit forms, individual hard copies are scanned in by submitting officials. These documents are uploaded, downloaded, signed, scanned, and uploaded again numerous times during the badging process, which involves multiple encryption/de-encryption processes that are cumbersome, time consuming and often ineffective. A long-time AOC COR reported that process frustration is compounded by a required manual checkmark of a single entry on the HSAA ID Request form (confirmation of the E-verify process), resulting in more unnecessary downloading, printing, and uploading. Final badge return also requires a manual portal entry for each employee. AOC professional personnel at the GS-13 and GS-14 level spend significant time on the administrative tasks associated with the HSAA process because the OCSO portal does not allow Contractors to submit requests or enter information themselves.⁸

⁸ Note: The OCSO Badge Portal is for the HSAA-issued Congressional IDs only. Because the USCP Unified IDs are not processed in an electronic system (and do not require OCSO to sign the CP-491) they are usually hand delivered to a project field office, signed by the COR and returned to the Prime Contractor (who then follows that same chain of emails/hard copies through subcontractors to field personnel).

AOC Badge Portal

We found that the AOC badge portal fails to provide for secure and efficient execution, monitoring and tracking of badging actions. It lacks automation and existing gaps in the notification system preclude visibility into badging status. This has resulted in considerable security vulnerabilities within the AOC as well as across coordinating badging entities.⁹ Portal processes are notification- rather than workflow-based, which adds to the lack of clarity on badging status. Further, the OCE reports that badge portal notifications for badge pickup approval are incorrectly communicated as actual pickup, which may never happen, further increasing portal data pollution. In addition, gaps in available data have hampered the production of useful reports from the portal, which indicates internal control deficiencies and a lack of auditability. The AOC, contractors, and other entities regularly rely on inconsistently sourced excel spreadsheets due to data silos. Finally, badge request processes were not administratively right-sized to their purpose; project personnel reported spending significant time on badging processes that were needlessly inefficient.

Portal processes are further hampered by locked fields on badge request forms, which prevent pre-filling prior to sending to vendors, who may lack computer access and therefore print and manually complete them. AOC badging personnel note that this is particularly burdensome for CORs, who have to re-type the returned information for portal submittal. The portal does not allow for the copying and pasting of data, so CORs have to retype the same information for each contractor, and although the portal has a dropdown list of contract numbers, it is not enabled to autofill, limiting

INADEQUATE PROCESSES FOR TRACKING OF SUBCONTRACT EMPLOYEES

Condition:

Jon Doe works for ABC Stone (a subcontractor to ABC Prime Systems) and receives a badge for the Russell Stone project. "ABC Prime Systems" is indicated on the issued badge rather than the company name ABC Stone. ABC Stone also has a subcontract for the Cannon Façade and is a subcontractor to XYZ Restoration for that project. **Note:** ABC Prime Systems has no relationship to the Cannon Façade project, thus creating a potential security issue.

Outcome:

Neither the HSAA form nor AOC badge portal processes address the complexities of AOC contract employee movement between projects. Jon Doe could be working on the Russell Stone project with a badge that displays the name of a company that is in no way affiliated with that project. Because contractors cannot access the portal, they cannot see all the badges they submitted, who else employs the worker, or their badge approval status.

Figure 2: Difficulties in tracking badges for contractors working on multiple projects

⁹ The lack of visibility into USCP HSAA systems results in CORs having no knowledge of USCP dates for when the employee reported for fingerprints and when the FBI background check was pulled and sent to OCSO. There is also no visibility for HSAA dates for ID issue (the portal only shows the date the employee was notified of suitable results and when they can go for ID Processing, actual ID pickup date is not provided, and there is often a discrepancy between "IDs Issued" and "IDs Approved." ID return dates are also problematic –ID's that are lost may be dropped in the mail and returned directly to the HSAA address on the badge. The HSAA may not notify the COR that the badge has been destroyed, creating another data/accountability gap.

its usefulness. Lastly, contractors are required to return their workers' badges to the COR, who must manually enter return dates in the portal for each employee.

Portal processes for recording and tracking contract and subcontract employees who move from project to project are particularly inadequate; these processes are largely reliant on communication between CORs and portal notations that are not mandated, electronically or otherwise. The HSAA ID request form requires the Prime Contractor name, rather than the actual company (subcontractor) that employs the worker.¹⁰ We were told by the OCE that this information must be tracked separately on spreadsheets, with the unrealistic expectation that it can be efficiently tracked by prime contractors, who may have as many as 500 workers. This problem worsens when employees switch subcontract firms because the prime may not be notified, leading to inaccurate tracking. The result is workers that are hard to trace for badge return. AOC badging personnel note that although the portal includes the subcontractor drop-down field, this is AOC-only information and the problem of tracking employees as they move from contract to contract is inadequately addressed. Figure 2 provides an example of difficulties in tracking badges for contractors working on multiple projects, and Figure 3 delineates how clear lines of COR accountability for badging erodes on Indefinite Delivery/Indefinite Quantity (ID/IQ) contracts in portal processes.

**OCE EXAMPLE FOR MULTIPLE PROJECTS
CONTRACT PERSONNEL**

"If you are on an ID/IQ project working on multiple contracts, you shouldn't be badged at the task order level, you should be badged at the parent overall IDIQ 5-year contract, and then with the understanding that you will be working on multiple projects. What really happens is that they usually get the badge from the first project they work on, and then just automatically get renewed every 2 years at Congressional changeover, and some people have been renewed probably 5, 6, 7 times, and you have no idea now where, okay, they're on the 30th project but they were badged back in 2010 by someone who's no longer even here. So that's one issue, multiple projects."

Figure 3: Erosion of lines of accountability for ID/IQ contracts

Finally, we also note that the OCSO, as the office of professional responsibility for badging, did not adequately meet its responsibility to implement a program that is effective, efficient and responsive to user needs and concerns. Although the OCE repeatedly raised concerns about portal software as significantly outdated, replete with data pollution and inaccurate notifications and that badging processes significantly hampered project efficiencies, these issues were inadequately addressed. Our concerns were enhanced by finding that the OCSO had limited awareness of Agency MOUs/MOAs with other Capitol complex badging entities, and information related to badge request and return in COR appointment letters is significantly outdated. The OCSO's general lack of program component awareness also raised

¹⁰ The USCP Unified IDs require the actual project name.

concerns that the USCP and HSAA may have limited awareness of the deficiencies in AOC's badging processes and their effect on the overall Capitol complex security.

Impact

As a result, the lack of an efficient and adequate badging process increased the probability for security vulnerabilities, criminality and process gaps within the AOC badging program. Responsibility for the management and tracking of badging functions is largely assigned to individual CORs and jurisdiction Points of Contact (POCs). This leaves the agency vulnerable to inconsistencies amongst those performing the process and may place too much responsibility for badging on jurisdictions. The decentralization of this function also lessens control of PII and places an undue administrative burden on the CORs and project managers of large projects. For AOC personnel who infrequently engage in the badging process, it requires a significant investment in learning for a function that may be little used.

In addition, costs to contractors resulting from inefficient badging processes may be covered through overhead rates or contract bids, resulting in Agency program costs that cannot be audited.

Conclusion

Identification and implementation of a state-of-the-practice security badging system will prevent gaps in accountability, reduce the need for numerous guidance and training venues, and provide assurance that the system is an effective component of Capitol complex security. Improved process and accountability measures will also enhance efficiency by limiting the number of users engaging in minor tasks or manual input of entries whose accuracy continually erodes. A state-of-the practice badging system would also provide the potentiality for task efficiency through automated reporting, rather than tasking jurisdiction POCs and project personnel with unnecessary and time-consuming administrative tasks.

Recommendation

Recommendation 2

We recommend that the Office of the Chief Security Officer, in coordination with the United States Capitol Police and the House Sergeant at Arms, perform a joint feasibility study to consider:

- a) Re-assigning signature authority for the CP-491 for the House of Representatives Sergeant at Arms-issued contractor badges from the OCSO to Contracting Officer Representatives, eliminating the hand carry of the CP-491 to USCP/Fairchild for Fingerprinting, and implementing the use of approval buttons or pdf secure signatures in place of manual signatures.

-
- b) Identification, development or acquisition of a badge management software solution that uses notification-based processes that ensures secure, efficient execution, monitoring and tracking of badging actions.

AOC Comment

While the AOC agrees it is important to improve the overall process and timelines related to completing CP-491 forms for House Sergeant at Arms (HSAA)-issued contractor badges, the ability to fully implement this recommendation is outside of the AOC's authorities. The responses to specific components of the recommendation are below:

- **Joint Feasibility Study:** The AOC will re-engage the Sergeants at Arms and the U.S. Capitol Police (USCP) regarding potential changes to existing badging systems. However, as noted during the exit conference, the AOC does not have the authority to compel legislative branch partners to modify existing processes or systems.
- **Re-assigning signature authority for the CP-491 for HSAA-issued contractor badges from the OCSO to Contracting Officer Representatives (CORs):** The AOC non-concurs with this recommendation due to the increased administrative burden to the existing process. Within the AOC, the assignment of CORs changes more frequently than the assignment of OCSO security specialists. Each change in COR would require approval by the Architect and an updated memo from the Architect to the HSAA and the Chief of the USCP listing the authorized requestors. In addition, the required training and administrative burden to keep the appropriate CORs aware of procedures and the near-constant updating of authorizations on file with the USCP and the HSAA would significantly increase the processing time for authorizations and cause further delays. The OCSO will continue to explore alternatives to the current process and will remain engaged in discussions with the HSAA and USCP points of contact on options to enhance the existing process.
- **Eliminating the hand carry of the CP-491 to USCP/Fairchild for fingerprinting:** Although there were discussions regarding automation of key components of the process at the beginning of the pandemic in 2020, the requirement to hand carry the CP-491 was not eliminated. The AOC will re-engage the USCP and HSAA regarding elimination of the hand carry requirement but cannot compel the change.
- **Implementing the use of approval buttons or pdf secure signatures in place of manual signatures:** The OCSO has no authority to compel the USCP or the HSAA to review or make changes to any internal processes to add approval buttons or secure signature methods on their forms. The OCSO will remain

engaged in discussions with the HSAA and USCP points of contact on options to enhance the existing process.

- Identification, development or acquisition of a badge management software solution that uses notification-based processes that ensures secure, efficient execution, monitoring and tracking of badging actions: The AOC has no authority to compel the USCP or the HSAA to develop or acquire a badge management software system that is compatible for all three agencies. The OCSO will coordinate with the AOC's Information Technology Division on potential solutions to improve the security and efficiency of the agency's internal processing of badging paperwork.

OIG Response

The OIG considers the recommendation unresolved. Although the AOC notes that it does not have authority over legislative branch partners, this response inadequately addresses current process gaps and inefficiencies in the security badging program that leave the AOC prone to an increased probability for future security issues and incidents. Employee names are not findable, status notifications are inaccurate, PII is unsecure, and lack of an HSAA/USCP/AOC shared system results in each component of the security badging program being vulnerable to inaccurate and outdated information. Ultimately, no badging entity is able to expeditiously report on who has authorized access to the Capitol complex, and information for any entity at any time could be outdated and inaccurate.

The OIG also recognizes that the AOC does not concur with re-assigning signature authority for the CP-491 for HSAA-issued contractor badges from the OCSO to CORs due to the increased administrative burden to the existing process. However, the OIG continues to recommend that the AOC work with other Capitol complex badging entities to develop an efficient and secure badging program, and its engagement in the proposed joint feasibility study. The OIG will monitor the program progress and follow up on the development of any action items and implementation of program improvements.

Finding 3

AOC Badge Security and Protection of PII

We found that the AOC security badge program lacked adequate security processes for protection of PII and physical badges.

This occurred because:

- There is inadequate oversight for badge request forms containing PII that progress through the AOC and HSAA approval process, along with minimal oversight for the protection of PII within and beyond the Capitol complex; and
- At employment termination, security badges may be returned via interoffice mail to non-secure locations, or not returned at all.

As a result, the lack of adequate security processes for badging activities increases the potential for security vulnerabilities and theft of PII within the AOC badging program.

Discussion

The AOC badge portal, located on the AOC intranet, provides guidance that describes the portal as a secure database for storing and protecting PII and as a place to view badge request status. This guidance also describes the portal as a location from which users can run reports for auditing but does not offer significant information about this reporting capability or who might use it. During our review, we found that the AOC security badge program lacked adequate security processes for protection of PII and physical badges. As badge request forms containing PII (social security numbers, dates of birth, etc.) progress through the AOC/HSAA approval processes, protection of PII within and beyond the Capitol complex is lax. This is due to inadequate accountability standards and a lack of oversight and inspection of actual practices. In addition, at termination, security badges may be returned via interoffice mail or hand delivered to non-secure locations, or not returned at all.

Security of PII

Badge portal processes require that ID request documents are uploaded, downloaded, signed, and scanned repeatedly during the badging process, with little-to-no accountability for the secure transmission of PII. During these processes, users create paper and digital copies and temporarily save emails with scanned attachments to network drives. There is no guarantee that users are shredding printouts or deleting scanned emails and files from temporary storage locations. During our evaluation, we found that there is inadequate oversight for badge request forms containing PII that

progress through the AOC and HSAA approval process, along with minimal oversight for the protection of PII within and beyond the Capitol complex. While AOC Order 4-16, Privacy Policy, controls for safeguarding of PII, there are no controls to ensure CORs and other AOC personnel are adhering to this policy, and the forms themselves pass through multiple layers of contractor/subcontractor personnel, at AOC's behest, with no AOC visibility or oversight.

There is also little written guidance for protection of PII during the badging process. Although the portal is described as "a secure database for storing and protecting Personally Identifiable Information," it was not implemented until 2015, and the formal guidance in Order 731-1 of 2012 and subsequent supplements make no mention of protection of PII. PII protection is not addressed in the portal use guide, and there is otherwise no formal guidance that addresses how to ensure the secure transmission of PII at the contractor/subcontractor level. PII is referenced on the last page of a FAQ on the portal site, but only to direct that encryption be disabled prior to loading documents. There is also an AOC notice on the rebadging process for new Congressional sessions, a biennial event, which directs issuers to "Ensure that any personal identifiable information (PII) is password protected when sending information within and/or outside of the agency. The password should always be sent in a separate email."

Interviews with jurisdictional badging points of contact revealed inconsistent processes for protection of PII (such as use of drop-boxes, encrypted emails and seven-zip files, information saved on personal drives, sealed envelopes sent via interoffice mail), which users have developed themselves, and direct knowledge of contractors and vendors not encrypting badging forms with PII returned for processing. While the OCSO reviews forms for completeness, the Agency has no visibility into protection of PII prior to their receipt.

Badge Return/Lost or Stolen IDs

At employment termination, badge portal guidance directs badges be returned to the OCSO, although in practice we found that they are often given directly to the HSAA. Security badges are returned in a variety of ways such as via interoffice mail, U.S. mail, or by hand delivery. In some instances, badges are not returned at all. Jurisdiction personnel reported that prior to final turn-in, badges may be left in non-secure locations, such as on the chair of a jurisdiction POC during the pandemic. Insecure and/or non-uniform badge return practices can also result in information gaps for timeliness and badge return dates, in part because the HSAA does not have access to the badge portal.

Portal guidance for lost or stolen IDs direct jurisdiction POCs to contact the HSAA for a Lost/Stolen ID Affidavit and Second ID Request forms. These are processed in the portal via a separate entry which requires the same information as initial requests, but they appear as Second ID requests. The number of Second ID Requests processed

for personnel reporting lost or stolen IDs was 57 in 2021; 20 in 2020; and 38 in 2019. Because the badges are the property of the U.S. House of Representatives, the AOC has little visibility into HSAA processes for lost/stolen IDs. The HSAA reported that while there is a level of concern about unreturned badges, it is not a high level of concern as badges get renewed every two years. During this evaluation, the OIG was unable to obtain records for the collection of fines for lost/stolen badges due to a lack of centralized recordkeeping for fine implementation. Enforcement measures for badge non-return are included in outboarding processes for AOC employees (a fine assessed via final paychecks), and via a special security clause in AOC contracts which requires a \$100 fine per unreturned badge.¹ There are no comparable controls for volunteers that are issued badges, such as those at the U.S. Botanic Garden, who do not return badges.

Impact

As a result, the lack of adequate security processes for badging activities increases the potential for security vulnerabilities and theft of PII within the AOC badging program. That the HSAA's biennial renewal is viewed as an internal control measure raises questions about how effective these badges are as a component of Capitol complex security. Weak internal controls for lost/stolen security badges have resulted in a lack of centralized recordkeeping for the collection of fines, inconsistent return processes and a lack of enforcement for a segment of the AOC badged population.

Conclusion

Revision and implementation of badging procedures and the oversight for security processes in the protection of PII and physical badges will help mitigate potential security vulnerabilities. Such measures will promote confidence in the protection of PII and accountability in the badging program.

Recommendation

Recommendation 3

We recommend that the Office of the Chief Security Officer develop and implement suitability policy language to include clear lines of responsibility and processes. Improvements should include:

¹ AOC clause 52.223-5: Special Security Requirements is included in Section G in all solicitations for services and in the Supplementary Conditions in all solicitations for construction when work is performed on the premises (excluding the United States Supreme Court premises). Item j of this clause states that "The contractor's failure to return any ID badge, access card, or key issued under this contract or order shall result in a deduction of \$100.00 from the contract per ID badge, access card, and/or key not returned."

-
- In the contractor suitability policy, assign the responsibility for the centralized recordkeeping of intra-agency badging agreement Memorandums of Understanding or Agreements to the OCSO; and
 - In both policies, guidance and requirements for secure badge return and protection and oversight of Personally Identifiable Information.

AOC Comment

The AOC concurs and will include responsibilities in the draft AOC Order 42- 7, Contractor Personnel Suitability Program Policy. This order applies to all persons who have access to AOC controlled grounds, facilities and information systems and includes AOC contractors, subcontractors and the employees of such contractors and subcontractors. The order will assign the responsibility for the centralized recordkeeping of intra-agency badging agreement Memorandums of Understanding or Agreements to the OCSO and requirements for secure badge return and protection and oversight of Personally Identifiable Information.

OIG Response

We reviewed the management comment and determined it addresses the finding and recommendation.

Finding 4

Interagency security badging communication processes were outdated and inadequate

We found inadequate badging information sharing between the AOC, the HSAA and the USCP, with reliance on outdated means of communication, with the potentiality of security gaps in notification as well as duplication of effort.

This occurred because:

- There are no shared communication, centralized tracking or recordkeeping systems amongst the Capitol complex entities (HSAA/USCP/AOC) that have a role in the processing of AOC contractor and employee badges; and
- Interagency communications are reliant on outdated processes such as quarterly emailing of badge status spreadsheets, and phone and email communications.

As a result, Capitol complex interagency badging processes remain inefficient and significantly vulnerable to security risks; there is little interagency

transparency for who has a badge, what stage of the badging process they are in, status of badge return, or timely communication about badges that are revoked for misconduct or other reasons. Furthermore, the inefficient and non-transparent information processes leave the AOC unable to effectively track or provide timely reporting of who has authorized access to the Capitol complex.

Discussion

We found inadequate badging information sharing between the AOC, the HSAA and the USCP, with reliance on outdated means of communication, and the potentiality for security gaps in notification as well as duplication of effort. There are no shared communication or recordkeeping systems amongst the Capitol complex entities (the HSAA/USCP/AOC) utilized in the security badging process for AOC. Communication between agencies is reliant on e-mailed reports and verification lists and phone

communications. This results in a lack of consistent interagency transparency regarding who has a badge, what stage of the badging process they might be in, if a badge has been returned, or if a badge was revoked due to misconduct or other reasons. AOC badging personnel noted that the lack of shared visibility leaves badge requesters with limited knowledge of actual badge status, and also results in significant waste and duplication of effort between agencies, with each manually entering the same data into three parallel systems (see Figure 4).

INCOMPATIBLE SYSTEMS

OCE Noted: "The biggest challenge with the existing Badging System, is that it is internal to AOC only (no visibility to contractors, USCP data, HSAA data), and a parallel system that we duplicate data entry in. The Contractors, USCP, and HSAA all maintain their own parallel systems that have similar data, but we do not have access to their data points (i.e., badge issued date, badge returned date) that is critical to accurate metrics/accountability/reporting. None of the data in our internal system is source data, it is essentially a giant excel table fed by individuals to produce reports."

Figure 4: Significant waste and duplication of effort

Interagency Communication of Badge Status

Overall, interagency communications on badge status are reliant on inefficient and outdated processes such as quarterly emailing of spreadsheets between AOC and the HSAA, and there is no centralized tracking of badge status amongst AOC/HSAA/USCP. The HSAA also has no visibility into the recipients of USCP issued site-specific badges, and the OCE noted there is a disconnect in the process between AOC and USCP; the USCP provides a notification that a person is cleared for badging, but does not issue a notification when the same individuals do not collect

their badges. Additionally, while the SSAA has no part in badging AOC employees, communications between the HSAA and SSAA also largely rely on thrice-daily reports sent for verification; the lack of shared system between the SSAA and HSAA creates an additional vulnerability to badge duplication.

Efficiency, security and reporting issues also arise due to the time it takes to get badged; the OCE noted that because tradespeople will not wait for the badging process if they find other employment, suitability checks are often performed for individuals who never report to AOC. Some subcontractors work around timeliness issues by submitting numerous applications for an eventual crew that is quite small, resulting in many more suitability checks than are necessary. The USCP does not report on the number of suitability checks it runs for construction site IDs or for the HSAA badges issued for AOC, and the HSAA also does not report how many badge requests are processed but never issued. Although the USCP did not express concern about the number of suitability checks they may be conducting unnecessarily, the lack of visibility or reporting for this merits review.

More importantly, although the USCP uses a system it refers to as the Badge Management System, which captures the photo and data of each person that receives a badge from USCP, this system's reporting functions appear to be inadequate. In attempting to respond to a Congressional data call after the events of January 6, 2021,² the AOC's OCE experienced significant difficulty in getting a timely and accurate accounting of badging data from the USCP. The information eventually received appeared to be manually compiled and was not initially adequate or accurate. The implications of this as an indicator of Capitol complex security as it relates to security badging are significant.

Lost/Stolen IDs

The HSAA processes for reporting lost/stolen IDs and requesting replacement IDs consist of the filing of an affidavit and Second ID request form. Because AOC badges are the property of the U.S. House of Representatives, as administered by the HSAA, the OCSO has no line of responsibility for follow-up actions once lost/stolen IDs are reported to the HSAA. The AOC/OCSO also have no visibility on the actions the HSAA takes for badges reported as lost/stolen. Once OCSO submits required paperwork to HSAA for a lost or stolen badge, they do not receive any further information from the HSAA. The OCSO tracks the number of lost/stolen IDs reported and engages in no further actions once paperwork is submitted to HSAA. OCSO was also not aware of any system of record maintained on confiscated IDs or employees trying to use old badges for access, and because the portal is designed as a site for the processing of badging applications, it does not accommodate additional actions such as tracking criminality, and no additional suitability checks are run on

² In a January 13, 2021, letter to Architect of the Capitol J. Brett Blanton, the Committee on House Administration requested "A complete, unredacted list of all AOC employees, interns, detailees, consultants and contractors as of December 6, 2020, and as of January 6, 2021."

AOC employees/contractors once they are hired. The lack of centralized authority and recordkeeping for the badging process significantly hampers AOC's ability to provide full accountability for its badges.

Impact

As a result, the Capitol complex intra-agency badging processes are inefficient and significantly vulnerable to security risks; there is little interagency transparency for who has a badge, what stage of the badging process they are in, status of badge return, or timely communication about badges that are revoked for misconduct or other reasons. There is also no centralized tracking of badge status. The inefficient and non-transparent information processes leave the AOC unable to effectively track or provide timely reporting of who has authorized access to the Capitol complex.

Conclusion

The fragmentation of badging entities and lack of an effective, modern communication system leaves the Capitol complex without a key security component. Although current security processes may work,³ they are reliant on phone and email communications and interagency cooperation rather than automated state-of-the-practice processes. Implementation of shared software can improve communication processes and enhance security.

Recommendation

Recommendation 4

We recommend that the Office of the Chief Security Officer in coordination with the U.S. Capitol Police and the House Sergeant at Arms, perform a joint feasibility study to develop and implement a centralized security badge management process through the use of shared software that allows for secure and efficient issuance, monitoring and tracking of badging actions, to include tracking and reporting of lost/stolen badges and follow-up actions.

AOC Comment

The AOC will continue discussions with legislative branch partners, but cannot commit to implementing this recommendation. The AOC has no authority to compel the USCP or the HSAA to develop or acquire a badge management software system that is compatible for all three agencies. Although a centralized system has been previously discussed, the identification, development or acquisition of a centralized security badge management software solution would require significant investments in personnel and information technology resources.

³ For example, in one instance a contractor removed for security reasons was flagged in the USCP system when that person applied to work on another contract, interagency communications about this were reliant on phone calls and email.

OIG Response

The OIG considers the recommendation unresolved. Although the AOC notes it does not have authority over legislative branch partners, we recommend the AOC work with other Capitol complex badging entities to develop an efficient and secure badging program, and that it engage in the proposed joint feasibility study. The OIG will monitor the program progress and follow up on the development of any action items and implementation of program improvements.

Observations

Outdated Badging Systems and Lack of Centralized Authority

AOC security badging processes are outmoded, ineffective and significantly lack security components that are standard for Executive Branch entities. Although there have been numerous efforts by the OCSO, the OCE and the Capitol Police Board working group to develop an improved badging process, these efforts have a history of faltering, with little progress made toward modernization of security components. Although the OCSO has made efforts to improve the AOC badging processes, the Agency's role as both tenant and steward of Capitol buildings leaves the OCSO without the authority to fully implement security credentialing best practices. The result is minor internal process improvements or desired improvements that are understandably centric to jurisdictional missions, which place efficiency at odds with security, rather than best practice solutions that respond to both.

Two recommendations in this report address implementation of a centralized security badging process developed in coordination with the USCP and the HSAA. This recommendation is supported by the numerous presentations made to Congressional oversight committees since the events of January 6, 2021, most of which reflect a need for significant funding and support for modernization and increased manpower for Capitol complex security.⁴ Security issues resulting from the lack of a common and modern badging system were starkly illustrated by the Agency's inability to efficiently respond to the Congressional data call regarding the events of January 6, 2021, as discussed earlier. Other security incidents also highlight inefficiencies in badging processes, such as when AOC project staff almost hired a contractor removed from another AOC project for conduct reasons. Although this was flagged by the USCP system, an AOC official noted that this was caught largely due to good

⁴ House Appropriations Subcommittee Hearing, Security of the Capitol Campus Since the Attack of January 6, 2021, Subcommittee on the Legislative Branch, January 11, 2022, retrieved from https://appropriations.house.gov/subcommittees/legislative-branch-117th-congress/congress_hearing; House Appropriations Subcommittee Hearing, Fiscal Year 2023 Budget Request for the United States Capitol Police, Subcommittee on the Legislative Branch, March 30, 2022, retrieved from https://appropriations.house.gov/subcommittees/legislative-branch-117th-congress/congress_hearing

working relationships between the AOC and USCP, with communications handled via phone calls and emails, rather than secure, automated processes. Another consideration to modernizing the badging system is the actual badge itself. USCP officers control access to most buildings in and around the Capitol complex and the primary security check for employee entry is a visual inspection of their ID. At the time of this report, the USCP did not employ building entry devices that scanned each employee to allow for rapid authentication and enhanced security for all physical and logical building access.

Issues of visibility and information sharing have also hampered the OIG's efforts to gather information on the planned improvements of other Capitol complex badging entities; both the HSAA and SSAA were unwilling to provide overviews of future upgrades and planned credentialing improvements. We were also unable to obtain information on vulnerabilities that may have led to a February 2022 security incident in a U.S. Senator's⁵ office. The OIG believes this indicates a future of continuing fragmented, insecure and inefficient processes. Interviews with staff, AOC officials and other badging entities revealed a consensus that future improvements will be incremental, largely agency-specific, and that a holistic, state-of-the-practice solution is not yet possible. In spite of this, our report includes a recommendation that Capitol complex badging entities "perform a joint feasibility study to develop and implement a centralized security badge management process." While the lack of visibility into planned improvements has contributed to the broad scope of this recommendation and hinders our ability to develop more targeted guidance,⁶ we believe that incremental and fragmented improvements to Capitol security credentialing will result in an ongoing waste of funds applied to Capitol security, and ongoing negative impacts to the efficiency and effectiveness of the AOC's programs and operations.

Best Practices

We identified some best practices that exist externally to the AOC that may enhance security badging program efforts across the Capitol complex. Specifically:

- Establish mandatory, Capitol complex-wide standards for a security badging program comparable to those prescribed by Homeland Security Presidential Directive 12 for the Executive Branch, to include the use of personal identity

⁵ <https://miamistandard.news/2022/02/28/fired-former-dianne-feinstein-staffer-entered-into-senators-office-smoked-blunt-in-smoke-filled-insurrection/>, retrieved on May 5, 2022

⁶ **Note:** In Congressional testimony provided in support of their FY2023 budget request, USCP Chief Thomas Manger noted that many of the requests were tied directly to Inspector General recommendations in reports produced in response to the events of January 6, 2021. In his testimony, Chief Manger stated the following: "In fact, as has been pointed out, this is the first budget that has been prepared since the IG reports have been completed, and many, if not most of the requests you will see in our FY23 budget submission are tied directly to the Inspector General's recommendations." We note this in support of the AOC OIG's need for adequate access to information necessary to the development of its recommendations.

verification (PIV) credentials.

- Establish the minimum requirement for PIV credential eligibility determination as a completed and favorably adjudicated Tier 1 investigation, (formerly called a National Agency Check with Written Inquiries).
- Establish standards for continuous vetting for maintaining PIV eligibility.

Appendix A

Scope and Methodology

We conducted this evaluation from November 2021 through June 2021, in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation (2020)*. These standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

This evaluation was self-initiated by the AOC OIG and was consistent with our 2021 agency Management Challenges that listed Balancing Security with Preservation as a Management Opportunity and Performance Challenge. Our objective for this evaluation was to assess the AOC's security badging process to determine if vulnerabilities exist within the program.

To address our evaluation objective, we reviewed relevant AOC policies and procedures related to the AOC's security badging program from Fiscal Years 2019 through 2021. We also reviewed AOC security badge records to establish if appropriate oversight measures were in place to report, track and account for security badges. Lastly, we conducted interviews with appropriate AOC, USCP and HSAA officials and staff to determine how security badge accountability and control processes and procedures are carried out in a day-to-day manner.

Use of Computer-Processed Data

We used computer-processed data in the performance of our work and determined that the data provided was sufficiently reliable to support any conclusions made from its use.

Prior Coverage

There was no prior coverage of the AOC's security badging program in the preceding five years.

Appendix B

Management Comments




Architect of the Capitol
U.S. Capitol, Room SB-16
Washington, DC 20515
202.228.1793
www.aoc.gov

United States Government

MEMORANDUM

DATE: July 12, 2022

TO: Christopher P. Failla
Inspector General

FROM: J. Brett Blanton 
Architect of the Capitol

SUBJECT: Response to Evaluation of the Architect of the Capitol's Security Badging Program (Project No. 2022-0001-IE-P)

The Architect of the Capitol (AOC) provides the following response to the subject Office of Inspector General (OIG) draft evaluation report:

Recommendation 1: We recommend the Office of the Chief Security Officer develop and implement a suitability policy for AOC employees and consolidate and implement revisions, as appropriate, to the current contractor suitability policy. Additionally, develop and implement a standardized timeline for policy revision and update within the current Fiscal Year.

AOC Response: The AOC concurs. The Office of the Chief Security Officer (OCSO) staff have completed coordination of the draft AOC Order 42-6, *Staff Personnel Suitability Program Policy*, with the Human Capital Management Division and are finalizing the associated forms. The draft order will enter the AOC's publication process no later than July 15, 2022. The OCSO has also drafted AOC Order 42-7, *Contractor Suitability Policy*, which will replace Order 731-1, *Contractor Suitability Policy*. The draft of AOC Order 42-7 will be entered into the AOC's publication process no later than September 1, 2022, after resolution of outstanding comments. The OCSO will conduct annual reviews of both orders no later than March 31st of each year.

Recommendation 2

We recommend that the Office of the Chief Security Officer, in coordination with the United States Capitol Police and the House Sergeant at Arms, perform a joint feasibility study to consider

- Re-assigning signature authority for the CP-491 for HSAA-issued contractor badges from the OCSO to Contracting Officer Representatives, eliminating the hand carry of the CP-491 to USCP/Fairchild for Fingerprinting, and implementing the use of approval buttons or pdf secure signatures in place of manual signatures.
- Identification, development or acquisition of a badge management software solution that uses notification-based processes that ensures secure, efficient execution, monitoring and tracking of badging actions.

AOC Response: While the AOC agrees it is important to improve the overall process and timelines related to completing CP-491 forms for House Sergeant at Arms (HSAA)-issued contractor badges, the ability to fully implement this recommendation is outside of the AOC's authorities. The responses to specific components of the recommendation are below:

- **Joint Feasibility Study:** The AOC will re-engage the Sergeants at Arms and the U.S. Capitol Police (USCP) regarding potential changes to existing badging systems. However, as noted during the exit conference, the AOC does not have the authority to compel legislative branch partners to modify existing processes or systems.
- **Re-assigning signature authority for the CP-491 for HSAA-issued contractor badges from the OCSO to Contracting Officer Representatives (CORs):** The AOC non-concurs with this recommendation due to the increased administrative burden to the existing process. Within the AOC, the assignment of CORs changes more frequently than the assignment of OCSO security specialists. Each change in COR would require approval by the Architect and an updated memo from the Architect to the HSAA and the Chief of the USCP listing the authorized requestors. In addition, the required training and administrative burden to keep the appropriate CORs aware of procedures and the near-constant updating of authorizations on file with the USCP and the HSAA would significantly increase the processing time for authorizations and cause further delays. The OCSO will continue to explore alternatives to the current process and will remain engaged in discussions with the HSAA and USCP points of contact on options to enhance the existing process.
- **Eliminating the hand carry of the CP-491 to USCP/Fairchild for fingerprinting:** Although there were discussions regarding automation of key components of the process at the beginning of the pandemic in 2020, the requirement to hand carry the CP-491 was not eliminated. The AOC will re-engage the USCP and HSAA regarding elimination of the hand carry requirement, but cannot compel the change.
- **Implementing the use of approval buttons or pdf secure signatures in place of manual signatures:** The OCSO has no authority to compel the USCP or the HSAA to review or make changes to any internal processes to add approval buttons or secure signature methods on their forms. The OCSO will remain engaged in discussions with the HSAA and USCP points of contact on options to enhance the existing process.
- **Identification, development or acquisition of a badge management software solution that uses notification-based processes that ensures secure, efficient execution, monitoring and tracking of badging actions:** The AOC has no authority to compel the USCP or the HSAA to develop or acquire a badge management software system that is compatible for all three agencies. The OCSO will coordinate with the AOC's Information Technology Division on potential solutions to improve the security and efficiency of the agency's internal processing of badging paperwork.

Recommendation 3: We recommend that the Office of the Chief Security Officer develop and implement suitability policy language to include clear lines of responsibility and processes. Improvements should include:

Architect of the Capitol

U.S. Capitol, Room SB-16 | Washington, DC 20515 | 202.228.1793 | www.aoc.gov

- In the contractor suitability policy, assign the responsibility for the centralized recordkeeping of intra-agency badging agreement Memorandums of Understanding or Agreements (MOUs/MOAs) to the OCSO; and
- In both policies, guidance and requirements for secure badge return and protection and oversight of Personally Identifiable Information.

AOC Response: The AOC concurs and will include responsibilities in the draft AOC Order 42-7, *Contractor Personnel Suitability Program Policy*. This order applies to all persons who have access to AOC controlled grounds, facilities and information systems and includes AOC contractors, subcontractors and the employees of such contractors and subcontractors. The order will assign the responsibility for the centralized recordkeeping of intra-agency badging agreement Memorandums of Understanding or Agreements to the OCSO and requirements for secure badge return and protection and oversight of Personally Identifiable Information.

Recommendation 4: We recommend that the Office of the Chief Security Officer in coordination with the U.S. Capitol Police and the House Sergeant at Arms, perform a joint feasibility study to develop and implement a centralized security badge management process through the use of shared software that allows for secure and efficient issuance, monitoring and tracking of badging actions, to include tracking and reporting of lost/stolen badges and follow-up actions.

AOC Response: The AOC will continue discussions with legislative branch partners, but cannot commit to implementing this recommendation. The AOC has no authority to compel the USCP or the HSAA to develop or acquire a badge management software system that is compatible for all three agencies. Although a centralized system has been previously discussed, the identification, development or acquisition of a centralized security badge management software solution would require significant investments in personnel and information technology resources.

Please feel free to contact Valerie L. Hasberry, Chief Security Officer, at valerie.hasberry@aoc.gov or 202.329.6121 if you have any additional questions.

Announcement Memo



Office of Inspector General
Fairchild Bldg.
499 S. Capitol St., SW, Suite 518
Washington, D.C. 20515
202.593.1948
www.aoc.gov

United States Government
MEMORANDUM

DATE: November 10, 2021

TO: J. Brett Blanton
Architect of the Capitol

FROM: Christopher P. Failla, CIG *C. Failla*
Inspector General

SUBJECT: Announcement for Evaluation of the Architect of the Capitol's (AOC's) Security Badging Program (2022-0001-IE-P)

This is to notify you that the Office of Inspector General is initiating an evaluation of the AOC's Security Badging Program. Our objective for this evaluation is to assess the badging process for AOC employees and contractors and determine if vulnerabilities exist within the program.

We will contact the appropriate AOC offices to schedule an entrance conference in the upcoming weeks. If you have any questions, please contact Audrey Cree at audrey.cree@aoc.gov or 202.631.2682, or Chico Bennett at chico.bennett@aoc.gov or 202.394.2391.

Distribution List:

Valerie Hasberry, Chief Security Officer
Jason Baltimore, General Counsel
Peter Bahm, Chief of Staff
Mary Jean Pajak, Deputy Chief of Staff

Acronyms and Abbreviations

AOC	Architect of the Capitol
CAO	Chief Administrative Officer
COR	Contracting Officer Representative
HSAA	U.S. House of Representatives Sergeant at Arms
ID	Identification
ID/IQ	Indefinite Delivery/Indefinite Quantity
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
OCE	Office of the Chief Engineer
OCSO	Office of the Chief Security Officer
OIG	Office of Inspector General
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POC	Point of Contact
SSAA	United States Senate Sergeant at Arms
SOP	Standard Operating Procedure
UCID	Unified Construction IDs
USCP	United States Capitol Police



OFFICE OF THE INSPECTOR GENERAL

Fairchild Building, Suite 518
499 South Capitol Street, SW
Washington, DC 20515
(202) 593-1948
hotline@aoc-oig.org