



UNITED STATES CAPITOL POLICE OFFICE OF INSPECTOR GENERAL

Performance Audit Building Access Card Process Report Number OIG-2013-03 January 2013

~~Important Notice - Distribution of This Document Is Restricted~~

~~This report is intended solely for the official use of the United States Capitol Police or the Capitol Police Board, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the United States Capitol Police or the Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~

UNITED STATES CAPITOL POLICE
WASHINGTON, DC 20003



INSPECTOR GENERAL

PREFACE

The Office of Inspector General (OIG) prepared this report pursuant to the Inspector General Act of 1978, as amended. It is one of a series of audits, reviews, and investigative and special reports prepared by OIG periodically as part of its oversight responsibility with respect to the United States Capitol Police to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the office or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The recommendations therein have been developed on the basis of the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.


I express my appreciation to all of those who contributed to the preparation of this report.

Carl W. Hoecker

Carl W. Hoecker
Inspector General

TABLE OF CONTENTS

	<u>Page</u>
Abbreviations	iii
Executive Summary	1
Background	2
Objective, Scope, and Methodology	2
Results of Performance Audit	4
Internal Controls	4
Compliance	6
Other Matters	6
Appendices	
Appendix A – List of Recommendations	10
Appendix B – Department Comments	11
Appendix C – BAC Process Narratives	12



Abbreviations

Architect of the Capitol	AOC
Building Access Card	BAC
Capitol Power Plant	CPP
Chief Administrative Officer	CAO
Contracting Officer	CO
Contracting Offer's Representative	COR
Fiscal Year	FY
Federal Acquisition Regulation	FAR
Generally Accepted Government Auditing Standards	GAGAS
Identification	ID
Illegal Immigration Reform and Immigrant Responsibility Act	IIRIRA
Information Technology	IT
Memorandum of Understanding	MOU
Office of Human Resources	OHR
Office of Information Systems	OIS
Office of Inspector General	OIG
Security Services Bureau	SSB
Standard Operating Procedures	SOP
United States Capitol Police	USCP or the Department

EXECUTIVE SUMMARY

At the request of the Chief Administrative Officer (CAO), the Office of Inspector General (OIG) and its contractor, Cotton & Company LLP, conducted a performance audit of the United States Capitol Police (USCP or the Department)'s Building Access Card (BAC) process. The objectives of this audit were to determine (1) if the Department had established adequate internal controls and procedures over USCP's badging and fingerprinting process to ensure that the risk of unauthorized personnel on the U.S. Capitol Complex was reduced to an acceptable level and (2) if USCP complied with applicable policies and procedures. The audit scope included controls, processes, and operations in place at USCP as of August 1, 2012.

Overall, we determined that internal controls and procedures over USCP's badging and fingerprinting process are adequate to ensure that individuals with a documented, adverse criminal history do not obtain BACs. However, we did identify areas that should be improved. Although USCP is not subject to the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), we recommend that the CAO continue current initiatives to develop and implement policies and procedures to incorporate the use of E-Verify and monitor contractor performance.

The USCP Badge and Fingerprint Office provides BACs for USCP contractors as well as Architect of the Capitol (AOC) Capitol Power Plant (CPP) contractors. USCP conducts background investigations for other legislative branch entities; however, those entities are responsible for making suitability determinations and issuing BACs. USCP's current policies and procedures for issuing BACs only require that the agency conduct a criminal background check before issuing a BAC to an individual. They do not require that the agency identify contractors and contractor employees that are not authorized to work in the United States and prevent them from obtaining access to or working at the Capitol campus. USCP's procurement policies also do not address the use of the E-Verify system.

In general, we recommend USCP make and implement a number of improvements in policies and procedures and adopt E-Verify. A complete list of all OIG recommendations is shown in Appendix A.

We provided a draft copy of this report to Department officials for comment on January 16, 2013. We incorporated the Department's comments as applicable and attached their response to the report in its entirety in Appendix B.

BACKGROUND

The United States Capitol Police (USCP or the Department) conducts background investigations through its Background Investigations Office, a section within the Office of Human Resources (OHR), as part of its hiring process. As the primary law enforcement agency of the legislative branch of the United States Government, USCP also conducts background investigations on potential employees for other legislative branch agencies. Generally, USCP's responsibilities include making inquiries regarding applicants' criminal history and providing this data to the requesting agency. The requesting agency then makes its own suitability determination and, if appropriate, issues a Building Access Card (BAC). However, USCP currently has a Memorandum of Understanding (MOU) with the Architect of the Capitol (AOC) under which USCP conducts the suitability determination for AOC's Capitol Power Plant (CPP) contractors and, if appropriate, issues their BACs. In accordance with the MOU, USCP conducts a criminal history check and, based on that information, determines if the applicant should receive a BAC for the CPP. USCP does not verify employment eligibility as part of this process.

Department guidance SOP [REDACTED] is intended to establish uniform guidelines for the issuance and replacement of identification cards and credentials. It identifies the purpose, definition, and procedures for obtaining a BAC. Department SOPs and Directives represent appropriate guidance for USCP.

In February 2012, the AOC OIG conducted an investigation and found that for one of the CPP subcontractors, five employees had social security numbers (SSN) that did not agree with the employees' names. USCP had issued BACs for three of these five employees. The other two employees had not applied for or received BACs from USCP. The AOC investigation determined that the contractor had not used E-Verify¹ to determine employment eligibility. Subsequent use of E-Verify uncovered the fraudulent information.

OBJECTIVE, SCOPE, AND METHODOLOGY

Through its contractor, Cotton & Company LLP, the USCP Office of Inspector General (OIG) conducted performance audit procedures over the USCP BAC process. These procedures were designed to ensure compliance and reduce the risk that unauthorized employees will be on site at the Capitol Complex. Specifically, we determined whether USCP:

¹ E-Verify is an Internet-based system that compares information from an employee's Form I-9, Employment Eligibility Verification, to data from U.S. Department of Homeland Security and Social Security Administration records to confirm employment eligibility. www.dhs.gov/e-verify.

1. Implemented adequate internal controls over USCP's badging and fingerprinting process to ensure that the risk of unauthorized personnel at the Capitol Complex is reduced to an acceptable level.
2. Complied with applicable laws, regulations, and guidance pertaining to the management and operation of the BAC process.

The scope of the audit included controls, processes, and operations in place at USCP as of August 1, 2012.

As part of our methodology, we obtained an understanding of USCP's BAC environment. We reviewed USCP policies and procedures and interviewed civilians and sworn officers involved in the BAC process to gain an understanding of the:

- Current structure and strategy, including how the BAC process supports the USCP mission
- Current BAC efforts underway
- Planned BAC efforts
- BAC policies and procedures
- Resources dedicated to BAC process
- Implementation of E-Verify tools
- Implementation of Federal Acquisition Regulation (FAR) language in new contracts

We also reviewed the organizational structure, the functionality of the BAC system, and relevant policies and procedures. We performed internal control reviews by documenting the workflow of each key process, BAC request, background investigation, adjudication, applicant interaction, and the controls governing each process. We observed, documented, and developed flow charts to graphically illustrate the following processes:

- BAC Request
- BAC Replacement – Lost or Stolen

We conducted this performance audit in Washington, DC from September through December 2012, in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States, 2011 revision, referred to as generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We provided a draft copy of this report to Department officials for comment on January 16, 2013. We incorporated the Department's comments as applicable and attached their response to the report in its entirety as Appendix B.

RESULTS

USCP has adequate internal controls over the BAC and background investigation process. However, our testing identified areas where controls should be strengthened. As a legislative branch agency, USCP is not required to comply with FAR, but has elected to do so. As FAR Section 22.18 requires agencies' contractors to be registered in E-Verify, USCP should therefore establish policies that address contractor utilization of E-Verify. USCP should also develop E-Verify policies regarding Department personnel, both civilian and sworn.

Internal Controls

USCP's objective with regard to the BAC and background investigation process is to establish uniform procedures for the issuance and replacement of identification cards and credentials. We determined that the current SOPs meet the documented USCP objective and that USCP has adequate internal controls over the BAC and background investigation process.

Building Access Card Policies and Procedures

USCP BAC SOPs/Directives² establish uniform procedures for the issuance and replacement of identification cards and credentials. They focus on obtaining credentials through the use of [REDACTED]. The majority of the document discusses procedures for Law Enforcement (sworn personnel) and USCP staff (civilian personnel) that have already undergone significant background investigations prior to and during the initial hiring process.

The [REDACTED] Directive³ [REDACTED]
[REDACTED] The purpose of this form is to determine if the applicant has a criminal history and ascertain whether it is suitable to grant them unescorted access on the Capitol Complex.

We noted no exceptions regarding the SOPs/Directives, as the documents were not intended to ensure compliance with the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA).

We reviewed MOU [REDACTED], which outlines the authority and procedures for USCP to conduct checks of criminal history upon request by other legislative branch agencies. The objective of these procedures is to ensure that in the interest of national security persons employed by and for the U.S. Congress shall be reliable, trustworthy, of good conduct and character, and of unswerving loyalty to the United States. Memo [REDACTED] between AOC and USCP, dated June 18, 2004, requires USCP to assume responsibility for suitability determinations and issue BACs to contract personnel requiring access to

² SOP [REDACTED]

³ Directive [REDACTED]

the CPP. USCP is in compliance with the MOU. The conditions, related to the CPP Renovation Project in 2004 that required USCP to assist AOC in its suitability determinations are no longer the same, however, as the power plant renovation project is complete. If a compelling reason no longer exists, then AOC should resume responsibility for performing suitability determinations and issuing BACs for CPP contractors.

Overall, we determined that USCP is in compliance with its current policies and procedures for conducting background investigations and issuing BACs. The USCP Badge and Fingerprint Office has controls in place to ensure that personnel with an adverse criminal history do not receive a BAC. However, our testing identified several clerical exceptions indicating that improvements are needed to ensure that all aspects of the process are consistently performed.

We obtained the population of badges issued in FY 2012 and selected a sample of 45 for testing. We tested the following control attributes:

- A. Had Form [REDACTED], been prepared?
- B. Had Form [REDACTED], been prepared?
- C. Was a copy of the applicant's ID included with the other documentation?
- D. Had the [REDACTED] been initialed by the ID staff?
- E. Was further adjudication acknowledged by a Sergeant?

All forms were present and complete, and we did not note any exceptions. However, we did note inconsistencies with respect to how the forms were completed and which version of the forms were used. For [REDACTED] we noted that the requestor did not fill in their printed name on 4 of the 45 samples reviewed. We also noted that CPP was using a different version of [REDACTED] version (04/11) than that being currently used by USCP. The CPP version did not include a space for the ID section staff to sign and date to indicate when the badge had been physically issued to the applicant. Adding a final review checklist to the bottom of the form would assist in ensuring the consistency of the information collected.

Recommendation 1: We recommend that USCP develop and implement policies and procedures for the Badge and Fingerprint Office to ensure that all forms are current, complete, and accurate. Specifically, USCP should:

- Add a checklist section to the bottom of Form [REDACTED] to document the procedures performed in reviewing the submitted form for completeness and accuracy.
- Update the USCP Directive [REDACTED] to require that agencies use the current Form [REDACTED] to document criminal history records check requests.

Control procedures tested included whether the Badge and Fingerprint Office's documentation contained a photocopy of the applicant's ID. All samples tested included

a copy of the ID; however, this procedure is not formal USCP policy. USCP should document this procedure as part of its policy. To enhance the control, USCP should also use a color copier and scan the ID so the data can be distributed electronically. USCP could further enhance this control by using an electronic system to validate the authenticity of applicant IDs.

Recommendation 2: We recommend that USCP evaluate the need for MOU [REDACTED] with respect to providing the BAC service for AOC CPP contractors.

Recommendation 3: We recommend that USCP update Badge and Fingerprint Office SOPs and Directives to require that IDs be copied/scanned. Additionally, USCP should consider using a color scanner/copier in place of the current black and white scanner/copier for improved readability.

Recommendation 4: We recommend that USCP consider the cost/benefit of using an electronic identification validation system.

Compliance

USCP is not subject to many of the laws and regulations that apply to executive branch agencies; however, USCP has adopted a policy to comply with the FAR, per Memorandum [REDACTED], dated September 20, 2011. USCP Acquisition Policy also includes procedures for following the FAR. We determined that USCP has not complied with this policy, however. Specifically, USCP contracts do not include language required by the FAR. FAR Section 22.18 requires contractors to utilize E-Verify, and FAR Section 52.222-54 provides the specific language to be included in affected contracts.

We obtained and examined a sample of USCP contracts to determine whether they included a clause requiring the use of E-Verify. Currently, USCP does not have an E-Verify requirement in any of its contracts, nor does it require its customer agencies to provide evidence that they utilize E-Verify. USCP stated their plan to adopt FAR clause 52.222-54, Employment Eligibility Verification, and include it in all contracts over \$150,000. The implementation date for this plan is January 1, 2013.

Recommendation 5: We recommend that USCP adopt FAR contract clause 52.222-54 and any similar clauses concerning Employment Eligibility Verification. Such clauses would affix responsibility to USCP contractors to enroll in E-Verify as a federal contractor and to use E-Verify to determine whether all new hires are eligible to work in the United States.

Other Matters

Employer Requirements

As an employer, USCP is required to prepare Form I-9, Employment Eligibility Verification. Employers are strongly urged by U.S. Citizenship and Immigration Services (USCIS) to enroll in and utilize E-Verify.

USCP has not communicated or coordinated E-Verify processes among federal agencies or within USCP organizations. Communication from the USCP Director of OHR states that USCP recognizes the additional control that the E-Verify tool can provide and has begun an initiative to deploy the tool within OHR.

Recommendation 6: We recommend that USCP develop and implement policies and procedures to facilitate OHR's use of E-Verify for USCP new hires.

Revised [REDACTED]

[REDACTED] is executed by both the applicant and an authorized requestor that is forwarded to the USCP Badge and Fingerprint Office, to initiate a criminal history records check.

We noted that USCP plans to revise form [REDACTED] to include country of citizenship and proof of work eligibility, such as passport number and country, for all foreign citizens requiring a badge.

We reviewed the current version and the new draft version of [REDACTED] and noted the following:

- The current version (04-11) is a one-page document with 25 sections for information.
- The draft version has 25 sections as well, but several lines were combined, allowing for two new questions: "Country of Citizenship" and "Document establishing identity from I-9 form."
- Each version of the form has three preparer sections. The first section is to be filled out by the applicant. The second section is to be completed by the authorized requestor. The third section is to be completed by the Identification Section personnel.

The "Country of Citizenship" question will corroborate the I-9 identity documentation. However, in order for the Identification Section to answer question number 25, "Document establishing identity from I-9 form," the Badge and Fingerprint Office must have a copy of the I-9 form on record. The revised [REDACTED] therefore includes new applicant instructions requiring the applicant to provide a copy of Employment Eligibility Verification Form I-9. The revised form also requires the requestor to attest to the statement, "I have verified that the applicant is authorized to legally work within the United States..."

The revised form depicts additional steps to verify employment eligibility. While the revised form clearly places the responsibility for providing the additional information on the applicant and the requestor, the fact that USCP is requesting copies of Form I-9 and the document establishing identity from the I-9 means that USCP is accepting additional responsibility for performing the employment eligibility verification procedures. This additional responsibility would also result in duplication of effort, since the requesting agency is required to perform these procedures as well. USCP should evaluate its role in

the BAC process to determine the value in conducting duplicate efforts that are the responsibility of the other entity's COR and/or its contractors.

Recommendation 7: We recommend that USCP carefully consider the implications of requesting additional information for the proposed new [REDACTED] such as Form I-9, Employment Eligibility Verification.

APPENDICES

List of Recommendations

Recommendation 1: We recommend that USCP develop and implement policies and procedures for the Badge and Fingerprint Office to ensure that all forms are current, complete, and accurate. Specifically, USCP should:

- Add a checklist section to the bottom of [REDACTED] to document the procedures performed in reviewing the submitted form for completeness and accuracy.
- Update the USCP Directive [REDACTED] to require that agencies use the current Form [REDACTED] to document criminal history records check requests.

Recommendation 2: We recommend that USCP evaluate the need for MOU [REDACTED] with respect to providing the BAC service for AOC CPP contractors.

Recommendation 3: We recommend that USCP update Badge and Fingerprint Office SOPs and Directives to require that IDs be copied/scanned. Additionally, USCP should consider using a color scanner/copier in place of the current black and white scanner/copier for improved readability.

Recommendation 4: We recommend that USCP consider the cost/benefit of using an electronic identification validation system.

Recommendation 5: We recommend that USCP adopt FAR contract clause 52.222-54 and any similar clauses concerning Employment Eligibility Verification. Such clauses would affix responsibility to USCP contractors to enroll in E-Verify as a federal contractor and to use E-Verify to determine whether all new hires are eligible to work in the United States.

Recommendation 6: We recommend that USCP develop and implement policies and procedures to facilitate the use of E-Verify by OHR for USCP new hires.

Recommendation 7: We recommend that USCP carefully consider the implications of requesting additional information for the proposed new [REDACTED] such as Form I-9, Employment Eligibility Verification.

DEPARTMENT COMMENTS



Phone: 202 224-5006

UNITED STATES CAPITOL POLICE

OFFICE OF THE CHIEF
119 D STREET, NE
WASHINGTON, DC 20510-7218

January 30, 2013

COPCOR 130083

MEMORANDUM

TO: Mr. Carl W. Hoecker
Inspector General

FROM: Kim C. Dine
Chief of Police

SUBJECT: Response to Office of Inspector General (OIG) draft report *Audit of Building Access Card Process at United States Capitol Police* (Report No. OIG-2013-03).

The purpose of this memorandum is to provide the United States Capitol Police response to the recommendations contained within the Office of the Inspector General's (OIG's) draft report *Audit of Building Access Card Process* (Report No. OIG-2013-03).

The Department agrees with all of the recommendations and appreciates the opportunity to work with the OIG to further improve upon current policies and procedures currently in place within the Department's badging process. The Department will assign Action Plans to appropriate personnel regarding each recommendation in effect to achieve long term resolution of these matters.

Thank you for the opportunity to respond to the OIG's draft report. Your continued support of the men and women of the United States Capitol Police is appreciated.

Very respectfully,

A handwritten signature in black ink, appearing to read "Kim C. Dine".
Kim C. Dine
Chief of Police

cc: Mr. Richard Braddock, Chief Administrative Officer
Thomas Reynolds, Assistant Chief of Police
USCP Audit Liaison

Nationally Accredited by the Commission on Accreditation for Law Enforcement Agencies, Inc.

BAC PROCESS NARRATIVES

General Overview

USCP Mission

The United States Capitol Police (USCP) was established as a federal law enforcement agency in 1828. USCP's primary responsibility is to protect and secure Congress; its Members, staff, and visitors; and the entire Capitol area from threats of crime or disruption by designing, implementing, and administering security systems and modalities that enable Congress to fulfill its Constitutional responsibilities in a safe and open environment. The Committee on House Administration and the Senate Committee on Rules and Administration provide legislative oversight of USCP. Annual budget requests are made to the Subcommittee on Legislative Branch in the House and the Subcommittee on Legislative Branch in the Senate.

Badge and Fingerprint and Background Investigations

USCP performs the criminal history checks for individuals who work on the Capitol Complex, including civilians, contractors, congressional staff, and sworn officers. USCP provides the Building Access Cards (BAC) for USCP, the Capitol Power Plant, and the Alternate Computer Facility. USCP does not make a suitability determination based on criminal history checks for individuals outside of USCP, the Capitol Power Plant, and Alternate Computer Facility. USCP conducts background checks on behalf of other agencies in the Capitol Complex, and the results are forwarded to the requesting agency for determination and adjudication. The other agencies have the equipment to produce their own BACs.

I. Budgeting and Planning for Core Mission Requirements

A. Budgeting

The budget for Background/Badge and Fingerprint is included with the budget for the Office of Human Resources, OHR Recruiting and Staffing. The Administrative Program Specialist prepares a Microsoft Word document and Microsoft Excel document for the budget submission. She or he submits the documents to the OHR Director. Once the Director has reviewed the documents, she or he submits them to a Budget Analyst. Afterward the budget is submitted to a Budget Office.

Items added to the budget must first be approved by the USCP Force Development Plan. The process for approval involves market research and justification. The chain of command for requests starts with the Supervisor of Support Services, then goes to the Background Investigations Section Commander, the OHR Director, the Chief Administrative Office, and finally to the Chief of Police, who approves the items for a specific fiscal year.

Within the budget for OHR, BOC 2610 contains the funds for Background/Badge and Fingerprint. In fiscal year (FY) 2013, BOC 2610 was allocated \$46,080, consisting of \$7,400 of General Office Supplies and \$38,680 of Credentialing/Badge and Fingerprint Supplies. The \$38,680 of Credentialing/Badge and Fingerprint Supplies included:

- \$1,200 for Laminating Pouches/Photo PLS Pouch
- \$1,800 for Sticky Backs
- \$7,000 for Lanyards
- \$5,500 for FARGO ID Printer Maintenance
- \$8,000 for Holograms
- \$2,000 for Credential Paper
- \$10,680 for Cartridges for Credential Printer/Printers
- \$500 for PVC Cards
- \$2,000 for Miscellaneous Machine Supplies

The machine that produces the credentials, [REDACTED] was recently put into service, and the new equipment was not budgeted in the traditional sense. USCP coordinates with the Congressional Identification Card Task Force to determine the badge management system that will be utilized throughout the Capitol Complex. The House, Senate, and USCP are each responsible for obtaining and deploying the selected equipment to ensure that credentials are consistent across the Capitol.

B. Strategic Plan

The USCP Strategic Plan FYs 2011-2015 (May 2012 Refreshed Edition) includes initiatives to harden access points, ensure the security of new and renovated buildings, and to develop and implement an improved functional alignment of OHR programs. Each of these initiatives could include elements of the BAC process; however, the strategic plan does not directly mention Badge and Fingerprint or the BAC process. Background investigation is included in the OHR Recruiting and Staffing section of the OHR budget, and Background Investigation would therefore fall under the Strategic Goal, Support the Mission, objective S.10. Human Capital.

II. Congressional Identification Card Task Force

The Congressional Identification Card Task Force meets on an as-needed basis to discuss matters before the task force. Meetings are primarily held prior to badge renewals (every two years, upon the sitting of a new Congress). The Congressional Identification Card Task Force is comprised of Badge Office Supervisors of the United States Capitol Police, House of Representatives, and the United States Senate. Its primary objective is to ensure consistency of credentials on the Capitol Complex. The Congressional Identification Card Task Force discusses/proposes changes to the Congressional Identification Cards on behalf of its own entity during the meetings; all proposals/recommendations are then up-channeled through the Chain of Command for internal approval and then forwarded to the Capitol Police Board, consisting of the Chief

of USCP, the House of Representatives Sergeant at Arms, the United States Senate Sergeant at Arms, and the Architect of the Capitol for final approval/denial.

III. Procurement

USCP does not have E-Verify clauses or requirements in any of its current contracts. According to the Procurement Office, USCP plans to evaluate the impact that the requirement may have on USCP contractors and on USCP itself. The target date for including E-Verify requirements in contracts is January 1, 2013. The Procurement Office plans to adopt FAR clause 52.222-54, Employment Eligibility Verification, and include it in all contracts. In addition to including the revised FAR language, USCP will need to design controls to monitor contractor compliance with E-Verify.

IV. Building Access Card Process

Criminal History Checks

USCP conducts the criminal history checks for individuals working in the Capitol Complex. Applicants must produce a photo ID and the proper paperwork, including Form [REDACTED]. The form must be completed and signed both by the individual applying for the BAC and by an authorized signer. Individuals with signature authority are listed on USCP's MOUs with its customer agencies. USCP staff in the Badge and Fingerprint Office verify that the signatures on [REDACTED] match the signature on the ID provided by the applicant and the signature of the authorized signer.

Once the Badge and Fingerprint Office has received and verified [REDACTED] it conducts a criminal history check. The criminal history check consists of two systems.

[REDACTED]
[REDACTED] If the individual is not applying for a USCP, Alternate Computing Facility, or Capitol Power Plant (CPP) badge, the results are forwarded on to the requesting agency, and USCP does not make a suitability determination on the results.

If the applicant is applying for a USCP, Alternate Computer Facility, or CPP badge and it is discovered that the individual has a warrant, the process stops. If the warrant is extraditable, the individual is arrested; if it is not extraditable, the individual is informed of the warrant. If the applicant has a criminal history, the results go to the Lieutenant of the Background Investigations Section for adjudication. USCP has implemented proprietary hiring standard operating procedures (SOPs) that are used to evaluate applicants. The Architect of the Capitol also provided USCP with an [REDACTED] to use for evaluating applicants who would be working at CPP. The adjudication criteria are proprietary data and are restricted to Law Enforcement personnel. In addition to the USCP SOPs and Architect of the Capitol [REDACTED], the Lieutenant considers how the criminal history relates to the position along with how recently the criminal

history occurred. Criminal history such as felonies and weapons charges automatically disqualifies an applicant. If the check comes back with no criminal record, the applicant can return in 24 hours to complete the BAC process.

The current [REDACTED] is undergoing revision and is expected to include additional requests for information to aid in documenting eligibility to legally work.

Building Access Cards

If an individual is applying for a USCP, Alternate Computer Facility, or CPP BAC, the applicant must submit Form [REDACTED], when they submit their photo ID and [REDACTED]. The requestor portion of the [REDACTED] must be completed and approved by a supervisor or management official from the requesting organizational element. If the applicant receives a favorable determination on their criminal history check, they return to have their photograph taken and badge created using the [REDACTED]. Upon being issued a badge, the individual signs the Form [REDACTED]. The form is also signed by the Badge and Fingerprint Office employee who issued the badge. The information from [REDACTED] is sent to the [REDACTED] drive, where the Chief of Police, Background Investigations, and OHR Director have access to it. New BACs will not work until a supervisor or management official contacts SSB to obtain access to secure areas for the badge.

Replacement Building Access Cards

When a BAC has been damaged and needs to be replaced, the holder must complete [REDACTED] and submit it to their USCP supervisor/sponsor for approval. The supervisor/sponsor reviews the form and, if approval is granted, returns the approved [REDACTED] to the holder. The holder then submits the approved [REDACTED] to the Badge and Fingerprint Office for issuance of the replacement BAC.

When a BAC is lost or stolen, the holder must immediately call the SSB System Operations Section so the card can be flagged or deactivated. If it is after hours, the holder must immediately report the lost or stolen card to the Watch Commander. The holder must then complete [REDACTED] and [REDACTED], and submit them to their supervisor for approval. The supervisor must then notify the Intelligence Section regarding the lost or stolen card and provide all pertinent information. The supervisor will review the forms and, if approval is granted, return the approved [REDACTED] and [REDACTED] to the card holder. The holder then submits the approved [REDACTED] and [REDACTED] to the Badge and Fingerprint Office for issuance of the replacement BAC.

[REDACTED]

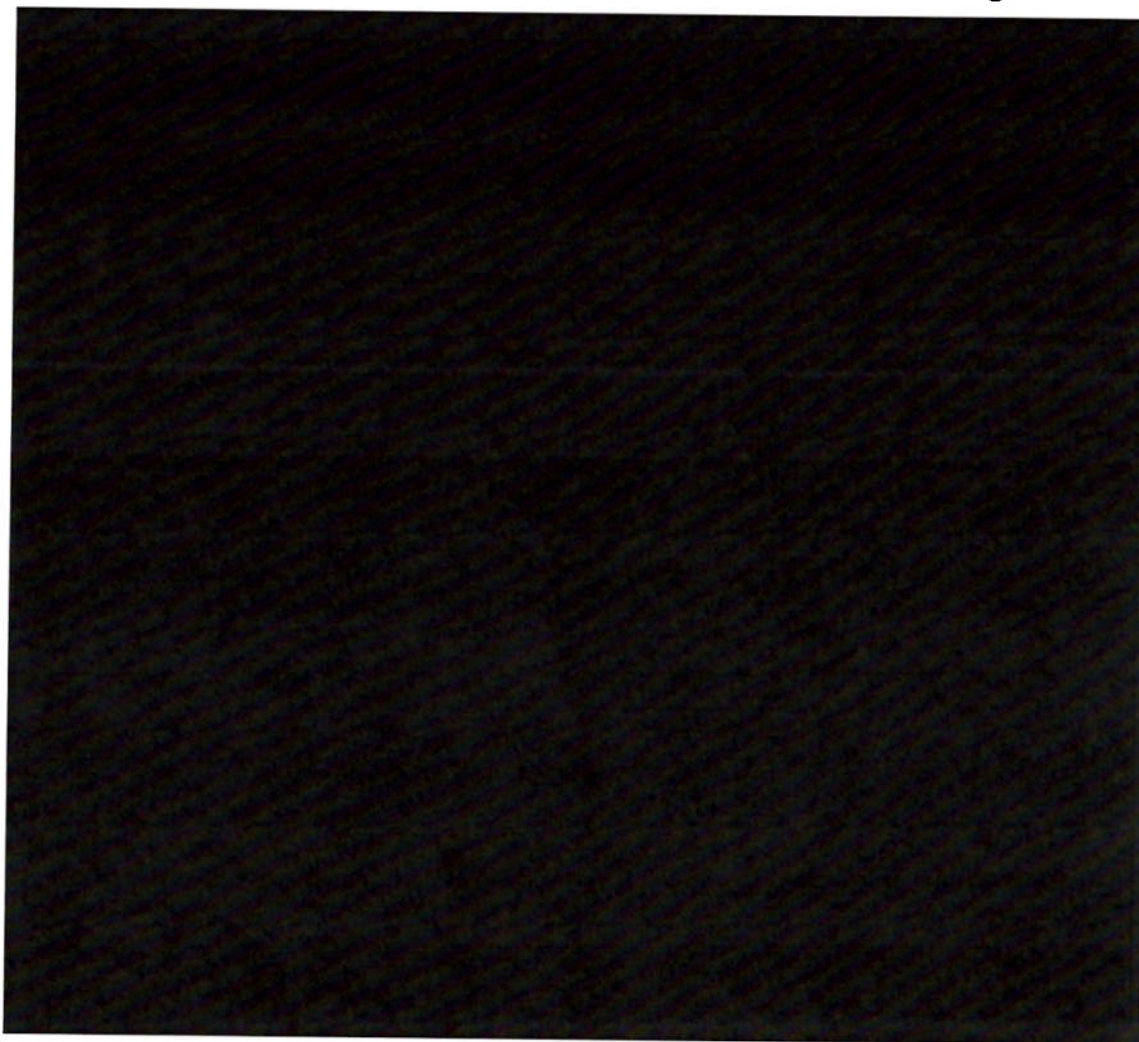
If the BAC is located or recovered before the holder is issued a replacement, all parties previously notified must be advised of the current status, any BOLO published must be rescinded, and any flagging/deactivation of the BAC must be lifted before the BAC can be used again.

Confiscated Building Access Cards

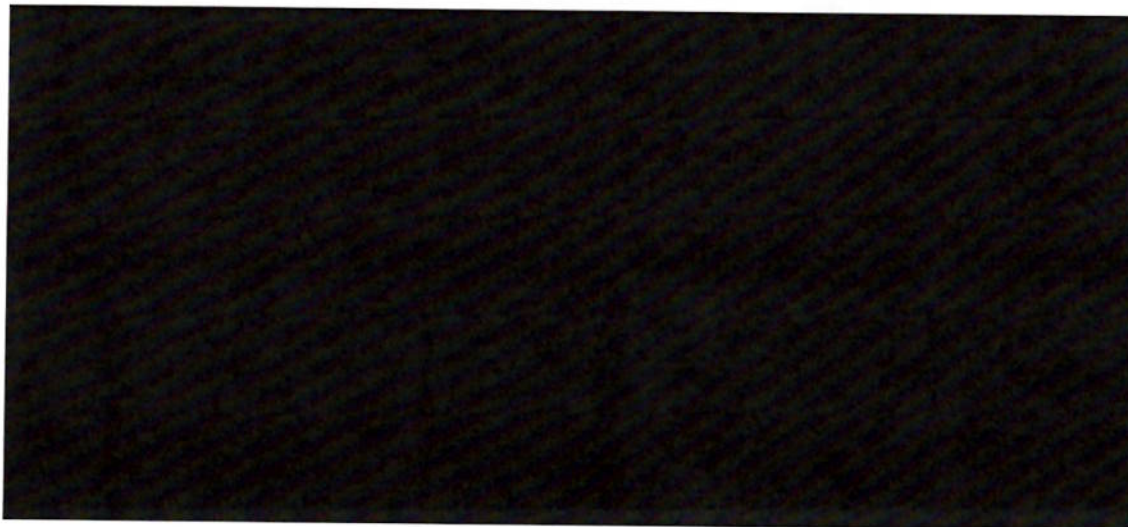
Sworn employees are required to confiscate BACs for the following reasons: the card is expired, the card is so damaged that the identity of the card holder or the validity of the ID can no longer be verified, the cardholder's employment has been terminated, or the person having possession of the card is not the person to whom the card was issued. Once a card has been confiscated, the sworn employee must report the confiscation by preparing Form [REDACTED], and Form [REDACTED] the confiscated card into the Form [REDACTED] and ensure the confiscation is entered into a log book. The sworn employee must then submit the appropriate reports and the confiscated card to a supervisor.

Types of Building Access Cards issued by USCP





Key Controls



- If an individual is applying for a USCP, Alternate Computer Facility, or CPP BAC, the applicant must submit Form [REDACTED], when they submit their photo ID and Form [REDACTED]. The requestor portion of the [REDACTED] must be completed and approved by a supervisor or management official from the requesting organizational element.
- Upon being issued a badge, the individual signs the Form [REDACTED]. The form is also signed by the Badge and Fingerprint Office employee who issued the badge.
- When a BAC has been damaged and needs to be replaced, the holder must complete Form [REDACTED] Building Access Card Replacement Request, and submit it to their USCP supervisor/sponsor for approval.
- When a BAC is lost or stolen, the holder must immediately call the SSB System Operations Section so the card can be flagged or deactivated. If it is after hours, the holder must immediately report the lost or stolen card to the Watch Commander. The holder must then complete Form [REDACTED] Request, and Form [REDACTED] and submit the forms to their supervisor for approval. The supervisor must then notify the Intelligence Section regarding the lost or stolen card and provide all pertinent information.

- Sworn employees are required to confiscate BACs for the following reasons: the card is expired, the card is so damaged that the identity of the cardholder or the validity of the ID can no longer be verified, the cardholder's employment has been terminated, or the person having possession of the card is not the person to whom the card was issued.
- Once a card has been confiscated, the sworn employee must report the confiscation by preparing [REDACTED], and Form [REDACTED]. The sworn employee must then insert the confiscated card into the Form [REDACTED] and ensure the confiscation is entered into a log book. The sworn employee must then submit the appropriate reports and the confiscated card to a supervisor.