Approved for public release (without appendices) by the Capitol Police Board on July 8, 2026

UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Survey of the United States Capitol Police Security Services Bureau

Report Number OIG-2015-11

September 2015

~~**IMPORTANT NOTICE**~~

~~**Distribution of this Document is Restricted**~~

~~This report contains sensitive law enforcement material and is the property of the Office of the Inspector General and is intended solely for the official use of the United States Capitol Police, the Capitol Police Board, or any agency or organization receiving the report 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

OFFICE OF 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 OIG prepares periodically as part of its oversight responsibility with respect to the United States Capitol Police (USCP) to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of a survey to learn more about the USCP Security Services Bureau (SSB) and to prepare for more detailed future work as part of our general oversight responsibility for the Department.

I express my appreciation to those contributing to the preparation of this report.

Fay F. Ropella
Inspector General

TABLE OF CONTENTS

	Page
Abbreviations and Acronyms	**ii**
Executive Summary	**1**
Background	**2**
Objective, Scope, and Methodology	**3**
Results	**4**
Overview of the Security Services Bureau	**4**
Potential Projects	**8**
Appendices	**11**
[redacted]	[redacted]

Abbreviations and Acronyms

Architect of the Capitol	AOC
Construction Security Division	CSD
Fiscal Year	FY
Government Accountability Office	GAO
House of Representatives	H.R.
[redacted]	[redacted]
Office of Inspector General	OIG
Office of Information Systems	OIS
Physical Security Division	PSD
Project Planning Section	PPS
Public Law	P.L.
Science Application International Corporation	SAIC
Security Services Bureau	SSB
Security Coordination Section	SCS
Security Equipment Section	SES
Sensitive Compartmented Information Facility	SCIF
System Operations Section	SOS
Technical Countermeasures Division	TCD
United States Capitol Police	USCP or Department

EXECUTIVE SUMMARY

In accordance with the Office of Inspector General (OIG) annual plan and as part of our general oversight responsibility for the Department, we conducted a survey of the United States Capitol Police (USCP or Department) Security Services Bureau (SSB) to assess its operations in order to better plan for future work. Our primary survey objective was to gain a better understanding of SSB, including the mission of its divisions and offices and define operational relationships between those offices and the Department. Our scope included divisions and offices, policies, and processes within SSB as of August 2015.

According to the USCP PoliceNet, SSB is responsible for the following services:

- Supervision and delivery of security surveys of congressional offices
- Potential locations for storage of national security information
- Design, installation, and maintenance of physical security systems
- Technical security countermeasures inspections

SSB provides physical and technical security for the Capitol Complex. Aligned under the Office of the Chief Operating Officer, SSB consists of three divisions: Construction Security Division (CSD), Physical Security Division (PSD) and Technical Countermeasures Division (TCD). As a main area of focus, PSD has four sections: Project Planning Section (PPS), Security Equipment Section (SES), Security Coordination Section (SCS) and System Operations Section (SOS).

In the Legislative Branch Appropriations Acts of 1996 and 1997, Congress transferred design, installation, and maintenance of security systems for the Capitol Complex from the Architect of the Capitol (AOC) to the Capitol Police Board and all of the related positions from the AOC to the Department. [redacted]

Future work for OIG could include audits, inspections, or evaluations of SSB for compliance with policies and procedures. SSB had not updated certain guidance since 2001. [redacted] According to the Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1, November 1999, a good control environment requires that

the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of Government resources, and achieving effective results. Control activities are also the policies and procedures, techniques, and mechanisms that enforce management's directives and, as such, help ensure management takes action that address risks.

As of July 9, 2015, SSB had a support staff of 102 contractors. The SSB Fiscal Year (FY) 2016 General Expenses budget request was approximately $20.2 million and included about $8 million, or 40 percent, for contract costs. Because OIG has identified acquisition management as a major management challenge for the Department for numerous years, potential future OIG work should include management of SSB contracts, which could identify internal control weaknesses, mismanagement, or fraud.

Other areas for potential audits include redundant services or resources resulting from the Department's decentralized information technology function. Separate information technology groups exist within the Department's Office of Information Systems (OIS) and SSB. While the environment for SSB has operational and security needs that differ from the environment that OIS oversees, inefficient use of resources may exist when SSB and OIS run parallel processes—such as vulnerability scanning. We requested and received comments on the draft of this report. Department officials suggested several technical changes that OIG incorporated where appropriate.

BACKGROUND

In 1995, the Capitol Police Board established a task force made up of representatives from the United States Secret Service and United States Capitol Police (USCP or Department) to review security for the Capitol Complex. The review included an analysis of deployed security technology. At the time of the task force review, the Electronic Engineering Division for the Architect of the Capitol (AOC), was responsible for the design, installation, and maintenance of security systems for the Capitol Complex. The task force recommended that security professionals design, install, and maintain the security technologies for the Capitol Complex. In its Legislative Branch Appropriations Act for 1996 (Public Law [P.L.] 104-53), Congress not only transferred design and installation of security systems for the Capitol Complex from AOC to the Capitol Police Board but also the related positions from the AOC to USCP. P.L. 104-53 required AOC approval for any alteration to a structural, mechanical, or architectural feature of the Capitol buildings and grounds required for a security system. Section 308(b) of P.L. 104-53 states:

> Effective October 1, 1995, the responsibility for design and installation of security systems for the Capitol buildings and grounds is transferred from the Architect of the Capitol to the Capitol Police Board. Such design and installation shall be carried out under the direction of the Committee on House Oversight of the House of Representatives and the Committee on Rules and Administration of the Senate, and without regard to section 3709 of the Revised Statutes of the United States (41 U.S.C. 5). On and after October 1, 1995, any alteration to a structural, mechanical, or architectural

> feature of the Capitol buildings and grounds that is required for a security system under the preceding sentence may be carried out only with the approval of the Architect of the Capitol.

In February 1996, Congress and the Capitol Police Board contracted with the Science Application International Corporation (SAIC) to review the organization and management approach of security support for the Capitol Complex. SAIC recommended that AOC transfer maintenance of security systems to the Department. In its Legislative Branch Appropriations Act for 1997 (P.L. 104-197), Congress not only transferred responsibility for maintaining security systems for the Capitol Complex from AOC to the Capitol Police Board but also the related positions from the AOC to the Department. P.L. 104-197 required AOC approval for any alteration to a structural, mechanical, or architectural feature of the Capitol buildings and grounds required for security system maintenance. Section 308(a) of P.L.104-197 states:

> Effective October 1, 1996, the responsibility for maintenance of security systems for the Capitol buildings and grounds is transferred from the Architect of the Capitol to the Capitol Police Board. Such maintenance shall be carried out under the direction of the Committee on House Oversight of the House of Representatives and the Committee on Rules and Administration of the Senate. On and after October 1, 1996, any alteration to a structural, mechanical, or architectural feature of the Capitol buildings and grounds that is required for security system maintenance under the preceding sentence may be carried out only with the approval of the Architect of the Capitol.

USCP placed the related positions from AOC into a new element within the Department, which became the Security Services Bureau (SSB).

OBJECTIVE, SCOPE, AND METHODOLOGY

In accordance with the Office of Inspector General (OIG) annual plan, we conducted a survey of SSB operations in order to better plan future work as part of our general oversight responsibility for the Department. Our primary objective was to gain a better understanding of SSB, including the mission of its divisions and offices and define operational relationships between those offices and the Department. Our scope included divisions and offices, policies, and processes within SSB as of August 2015.

To accomplish our objectives, we interviewed SSB officials to gain an understanding of the organization. We reviewed available standard operating procedures and directives related to SSB, including those in draft form. [redacted] We also reviewed SSB's budget, projects, staffing, and contract information. Additionally, we researched and reviewed information related to the history of SSB. Furthermore, we reviewed both past and current OIG audits related to SSB as well as an information paper prepared by SSB in response to a past audit. And, we reviewed guidance from the Government Accountability Office (GAO).

We conducted this survey in Washington, D.C., from June through August 2015 under the authority of the Inspector General Act of 1978, as amended. We did not conduct an audit, the objective of which would be the expression of an opinion on SSB programs. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have

come to our attention that would have been reported. ~~This report is intended solely for the information and use of OIG and USCP and is not intended to be and should not be used by anyone other than the specified party.~~

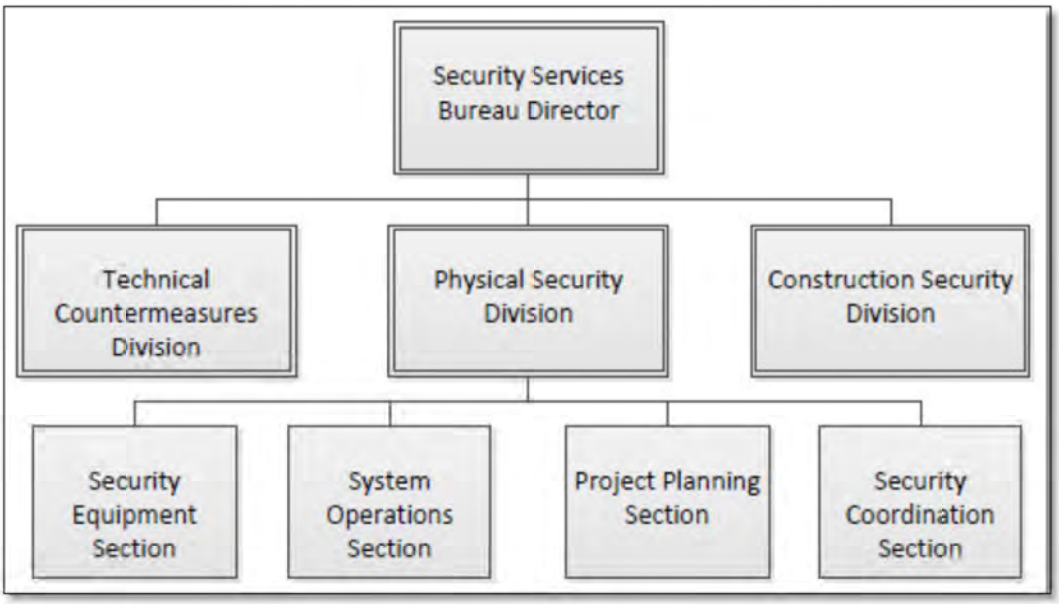
RESULTS

OIG gained a better understanding of the history of SSB, including the mission of each division and office within SSB and operational relationships between those offices and the Department. As a result of this limited survey, OIG identified future work related to SSB, such as compliance with policies and procedures, management of contracts, and information technology management.

Overview of the Security Services Bureau

SSB provides physical and technical security for the Capitol Complex. Aligned under the USCP Chief of Operations, SSB consists of three divisions: Technical Countermeasures Division (TCD), Physical Security Division (PSD), and Construction Security Division (CSD). As shown in Exhibit 1, PSD has four sections: Project Planning Section (PPS), Security Equipment Section (SES), Security Coordination Section (SCS), and System Operations Section (SOS).

Exhibit 1 – Organization Chart of the Security Services Bureau



Source: OIG generated using information provided by Department officials and PoliceNet.

[redacted]

[redacted]

CSD is primarily responsible for overseeing the security of construction projects on the Capitol Complex. The division collaborates with the AOC and with internal PSD sections in order to develop plans for the security at construction sites. CSD oversees the implementation of physical security plans and coordinates with other divisions within the Department to make recommendations on the appropriate manpower for construction security to the Assistant Chief of Police. CSD coordinates access, deliveries, and screenings for vehicles and materials related to construction activities The division is also responsible for security of the Alternate Computer Facility (ACF) and assists with constructing security fencing for large events. CSD also maintains a log listing every construction project occurring in the Capitol Complex and notifies the Department of any upcoming construction.

PSD is made up of four sections—PPS, SCS, SES and SOS—that are responsible for the security systems of the Capitol Complex.

PPS is primarily responsible for designing and engineering security systems. It also replaces existing security systems as part of large life-cycle projects. Bureaus and/or divisions usually schedule large life-cycle projects years in advance. PPS not only designs and updates existing security systems, but it also designs and constructs new security systems. In addition, the section oversees installation contractors, coordinates security systems and equipment for Members of Congress, assesses drawings for new and existing security systems and equipment, and coordinates guidance for any new security systems for the Complex. SCS notifies PPS of new security system projects. After SCS completes a security assessment and the Assistant Chief of Police approves its recommendations, SCS notifies PPS of the project so it can begin planning.

SCS is primarily responsible for security assessments of Member district offices and residences. SCS also conducts ad-hoc assessments of specific spaces on the Capitol Complex by request if the respective Sergeants-at-Arms and Assistant Chief of Police approve the request. SCS forwards all recommendations from its assessments on the Capitol Complex to the Assistant Chief of Police for approval. If the Assistant Chief of Police approves the recommendations, SCS forwards them to PPS for project planning and installation. The section installs, calibrates, and tests security screening equipment used for special events. In addition, SCS provides upkeep and maintenance for magnetometers, barriers (Figure 1), and other security equipment throughout the Complex. The section serves as a liaison with other members of the Department, outside law enforcement agencies, and other organizations. SCS conducts [redacted] physical security surveys of congressional buildings.

Figure 1 – Vehicle Barrier

Source: USCP.

SES is primarily responsible for small installations and maintenance of security systems. The section handles on-call operations and services for security systems. It also keeps track of work orders and projects, as well as evaluates the condition of physical security equipment. The section evaluates available physical security equipment for possible use on the Complex. SES advises PPS of failing security systems that may need upgrading, and coordinates installations and alterations of systems with SOS. SES coordinates with AOC and contractors for the maintenance and installation for physical security systems and testing and certifying installations. To track and document maintenance of security equipment for which it is responsible, SES uses a program called the [redacted].

SOS is primarily responsible for the oversight and management of the SSB security network and all security system programming, ensuring that data are up to date and accurate before activating a system and implementing client access requests. The section ensures that changes to the security system do not affect the infrastructure of the system; thereby ensuring that data for the alarm systems and access control devices are current. SOS maintains the SSB Security Network, which includes programming and monitoring podium computers; programming and maintaining the camera systems; programming and updating the duress system; and creating/maintaining maps for access control and duress.

The FY 2016 General Expenses budget request for SSB was $20,205,647 and included $8,211,740, or 40 percent, for contract costs. As of June 26, 2015, SSB had 47 employees and 14 vacancies, [redacted]. As of July 9, 2015, SSB used 102 contractors as support staff.

[redacted]

[redacted]

[redacted]

Potential Projects

OIG identified issues suitable for future evaluations, inspections or audits. Specifically, SSB had not updated certain guidance since 2001. [redacted] The SSB General Expenses budget request of approximately $20.2 million for FY 2016 included about $8 million, or 40 percent, for contract costs. Because OIG has identified acquisition management as a major management challenge for the Department for numerous years, potential future OIG work should include management of SSB contracts, which could potentially identify internal control weaknesses, mismanagement, or fraud. Other areas for potential audits relate to the Department's decentralized information technology management. Audits of those areas could result in increased effectiveness and efficiency of operations—including improved use of the Department's resources.

Outdated Policies and Procedures

GAO *Standards for Internal Control in the Federal Government; Documentation of the Internal Control System*, GAO-14-704G, September, 2014, states:

> Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

> Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

SSB had not updated certain guidance since 2001. [redacted] In addition, [redacted] Future evaluations, inspections, or audits could determine SSB compliance with such guidance and examine whether its policies and procedures are effective and/or accurately reflect its current processes.

Acquisition Management

GAO *Standards for Internal Control in the Federal Government,* GAO-14-704G, September, 2014, states:

> Management may engage external parties to perform certain operational processes for the entity... Management, however, retains responsibility for the performance of processes assigned to service organizations. Therefore, management needs to understand the controls each service organization has designed, has implemented, and operates for the assigned operational process and how the service organization's internal control system impacts the entity's internal control system.

As of July 9, 2015, SSB had a support staff of 102 contractors. The SSB FY 2016 General Expenses budget request included $8,211,740 for contract costs. A future evaluation, inspection, or audit of SSB contracts could identify potential internal control weaknesses, mismanagement, and/or fraud.

Information Technology Management

According to OIG Report Number OIG-2012-01, *Independent Audit of USCP Enterprise Architecture,* issued December 2011, the Department's information technology management is decentralized. Separate information technology groups exist within the Department's Office of Information Systems (OIS) and SSB. According to the Information Paper [redacted], dated December 12, 2011, industry standards and best practices recommend isolating security networks to deter outside attacks. Combining the SSB network with the OIS-supported network would not only be difficult but also increase the security network's vulnerablility and possibility of failure.

An ongoing performance audit of the Department's information security program revealed that the SSB environment has different operational and security needs than the environment OIS oversees. However, while a need exists for a variety of protections and information security controls over different systems and environments, use of resources may not be efficient when both SSB and OIS run parallel processes such as vulnerability scanning. Future audits in this

area could potentially identify other processes with duplication of effort resulting in a better use of resources and more efficient and effective operations.

CONTACTING THE OFFICE OF INSPECTOR GENERAL

Success of the OIG mission to prevent fraud, waste, abuse, or mismanagement depends on the cooperation of employees and the public. There are several ways to report questionable activity.

Call us at 202-593-3868 or toll-free at 866-906-2446. A confidential or anonymous message can be left 24 hours a day/7 days a week.

Toll-Free
1-866-906-2446

Write us at:
United States Capitol Police
Attn: Office of Inspector General, Investigations
119 D Street, NE
Washington, DC 20510

Or visit us – we are located at:
499 South Capitol Street, SW
Suite 345
Washington, DC 20003

You can also contact us by email at: OIG@USCP.GOV

When making a report, convey as much information as possible such as: Who? What? Where? When? Why? Complaints may be made anonymously or you may request confidentiality.

Additional Information and Copies:

To obtain additional copies of this report, call OIG at 202-593-4201.

OFFICE OF
INSPECTOR GENERAL
UNITED STATES
CAPITOL POLICE
INSPECTOR GENERAL