UNITED STATES CAPITOL POLICE
WASHINGTON, DC 20003

January 24, 2012

INSPECTOR GENERAL

MEMORANDUM

TO: Chief of Police – Phillip D. Morse, Sr.

FROM: Inspector General – Carl W. Hoecker Carl W Hoecker

SUBJECT: *Management Letter Related to the Audit of the United States Capitol Police's Fiscal Year 2011 Financial Statements* (Report No.OIG-2012-03)

This management letter related to the audit of the United States Capitol Police's (USCP) fiscal year 2011 financial statements is attached for your review and action. This management letter, prepared by Clifton Gunderson LLP (CG), an independent external auditor, discusses a number of internal control deficiencies that were identified during the audit of the financial statements. These control deficiencies, if addressed, could enhance the efficiency and effectiveness of internal controls.

In the view of CG, these deficiencies, although of concern, did not rise to the level necessary to be included in the report on the financial statement audit. In their response, the Department indicated that it did not have any additional comments beyond those that were provided on the Notices of Findings and Recommendations (NFR) during the audit. Therefore, CG has incorporated a summary of management's comments to the NFRs in the management letter.

Since CG made and reported these comments in a management letter rather than within material weakness or significant deficiency framework, the Office of Inspector General will not track these recommendations through its formal compliance process. However, the financial statement auditors will evaluate compliance during future audits of USCP's financial statements.

If you have any questions, please call me at [redacted] or Fay F. Ropella, Assistant Inspector General for Audits, at [redacted]

Attachment: As stated.

cc: The United States Capitol Police Board
Deputy Chief Thomas P. Reynolds, Chief of Operations
Mr. Richard Braddock, Chief Administrative Officer
[redacted] Clifton Gunderson LLP
[redacted] Audit Liaison (5 copies)

Management Letter Related to the Audit of the United States Capitol Police Fiscal Year 2011 Financial Statements

Report No. OIG-2012-03

Clifton Gunderson LLP
Certified Public Accountants & Consultants
4250 N. Fairfax Drive, Suite 1020
Arlington, Virginia 22203
(571) 227-9500

Clifton
Gunderson LLP
Certified Public Accountants & Consultants

Inspector General
United States Capitol Police

Chief of Police
United States Capitol Police

United States Capitol Police Board

We (Clifton Gunderson LLP[1]) have completed our audit of the United States Capitol Police (USCP) financial statements as of and for the year ended September 30, 2011, and have issued our report dated November 21, 2011 (Report No. OIG-2012-02[2]). In connection with our audit, we noted matters that present opportunities for strengthening internal and compliance controls. We summarized our comments and suggestions regarding these matters in this letter, which includes USCP's responses to the draft comments and suggestions.

We previously issued our report on USCP's internal control as of September 30, 2011 in our report dated November 21, 2011. This letter does not affect our report dated November 21, 2011 on USCP's fiscal year 2011 financial statements.

We have discussed these comments and suggestions with USCP personnel and, if necessary, we will be pleased to discuss them in further detail at your convenience.

This report is intended solely for the information and the use of the management of USCP and the USCP Inspector General and is not intended to be and should not be used by anyone other than these specified parties.

Clifton Gunderson LLP

Arlington, Virginia
November 21, 2011

[1] Clifton Gunderson LLP merged with LarsonAllen LLP effective January 2, 2012 and the firm became known as CliftonLarsonAllen LLP.

[2] *Indpendent Auditor's Report on the United States Capitol Police, 2011 Financial Statements* (OIG-2012-02, December 2011).

United States Capitol Police
Fiscal Year 2011 Financial Statements Audit

Management Letter
Report No. OIG-2012-03

Table of Contents

I. Introduction

During our audit, we provided USCP management with 17 Notices of Findings and Recommendations (NFRs) related to the fiscal year (FY) 2011 financial statements audit. A NFR is a written communication of an issue identified during the audit. Each NFR includes a description of the finding or issue, criteria, cause, and recommendation for management. Each NFR has a section for management's response and its concurrence and non-concurrence with the finding and recommendation. The NFRs were provided to USCP management for their review and response.

Each NFR is categorized as a Material Weakness, Significant Deficiency or Management Letter Comment. A NFR that is categorized as a Material Weaknesses or a Significant Deficiency is included in our separate report titled Independent Auditor's Report on Internal Control dated November 21, 2011. The NFR categorized as management letter comment and USCP's response are included in this letter.

The predecessor auditor did not issue a management letter for the FY 2010 financial statements audit.

II. Management Letter Comments

1. Untimely Review of Fund Balance With Treasury (FBWT) Related Reconciliation and Reports (New Finding)

During our internal control testing for FBWT, we reviewed three monthly reconciliations between the U.S. Treasury's Government Wide Accounting (GWA) Account Statement and the USCP's [redacted] general ledger 1010 account. The March 2011 monthly reconciliation was completed and signed by the preparer on 4/21/2011 but not approved by the Deputy Director of the Office of Financial Management (OFM) until 9/9/2011, five months beyond the completion of the reconciliation itself.

We also noted the [redacted] for the month of March 2011 was reviewed, as evidenced by the Lead Accountant's signature, 1 day after the report was submitted.

[redacted] *Section 1.5* requires timely approval of the FBWT reconciliations.

In addition, [redacted] *Section 1.4* requires review and approval of the draft SF 224 before submission in the GWA system.

Recommendation:

We recommend the Office of Financial Management enforce implementation of its policies and procedures.

Management Response:

"We concur and have already made re-assignments of tasks to ensure timely review of FBWT related reconciliations and reports."

2. Untimely Vendor Payments (Prior Year Finding 2.7)

During the internal control testing of non-payroll disbursements, we noted 12 of 45 invoices tested were not paid in a timely manner (within 30 days from receipt of the invoice). Payments ranged between 33-121 days following invoice receipt.

It is a best business practice to adopt procedures to ensure timely payment of invoices.

Recommendation:

We recommend USCP establish a due date for making payments after receipt and approval of an invoice and develop procedures to ensure adherence to this date.

Management Response:

"We concur and will develop procedures to ensure immediate notification of FLOs upon receipt of invoices and strengthen our follow-up to FLOs for delinquent receiving documents within our financial management system."

3. Incomplete Government Purchase Card Certification Form (New Finding)

One of four sample items tested for the Government Purchase Card Certification Form was not signed by the USCP Approving Official and/or the USCP Program Manager. Furthermore, the Delegation of Authority section was not signed by the Head of the Procurement Division.

The USCP Purchase Card Guide Standard Operating Procedures requires that before a purchase card can be issued to an individual card holder, certification statements must be attested to by the Card Holder, the Approving Official, the Program Coordinator, and the Procurement Officer.

Recommendation:

We recommend USCP maintain current Delegation of Authority forms for all purchase cardholders and establish a process to ensure all required signatures are present on the form.

Management Response:

"The Procurement Division concurs with this recommendation and will establish a process to review Purchase Card files and to ensure that all required signatures are present on all forms."

4. Lack of Fleet Card Program Training (Prior Year Finding 2.13)

The USCP has not fully implemented a comprehensive training program for its fleet card coordinators and potential users of the vehicles. During fiscal year 2011, the Procurement Division began developing a Fleet Card Annual Training Program (program). However, the program had not been finalized as of 11/16/2011. Moreover, we requested but were not provided with a list of fleet coordinators.

GAO *Standards for Internal Control in the Federal Government* states "A positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment. Good human capital policies and practices are [one] critical environmental factor. This includes establishing appropriate practices for...training...personnel."

Recommendation:

We recommend the CAO finalize the annual fleet card training program and ensure appropriate training is provided timely and documented for tracking and monitoring purposes.

Management Response:

"The Procurement Division concurs with this recommendation and will implement fleet card coordinator training and will maintain records of training completed." The names of fleet coordinators were also listed in management response. However, we did not include the names in this response.

5. Lack of Justification for Vendor Additions and Modifications in [redacted] (Prior Year Finding 2.9)

Our review of USCP procurement controls revealed the form to request current vendor addition or modification is not accompanied by proper approval or justification. Additionally, [redacted] has not been updated with the timeline for performing semi-annual review of vendor additions and modifications.

Directive [redacted] includes language for the Lead Systems Accountant or Accounting Officer to perform a review of vendor processing performed by those who hold the role of System Administrator in [redacted] However, there is no specific language as to the timeline of which the review is to be performed. Section 1.4 – Authorized Personnel of the directive states that "All request to change a vendors name or TIN must be approved by Procurement Division staff". Section 1.6 – Process to Request/Modify an FMS Vendor Code, states "Creation of a new vendor record due to either a vendor name changes or taxpayer ID number will be approved by Procurement Division staff."

Recommendation:

We recommend the CAO modify [redacted]o include a timeframe for the semi-annual review of vendor additions and modifications. We also recommend the CAO strengthen the approval process of the vendor enrollment forms to include maintaining email approval of adding/modifying the vendor in addition to maintaining the form. The email should be clear as to who is being approved, and the effective date and other details or reference to the form number or form reference number so both documents can be tied together.

Management Response:

"We concur and will update Directive [redacted] to include specific timeframes for semi-annual review of vendor additions and modifications. In addition, emails from approver will be maintained as supporting documentation of approving adding/ modifying the vendor in addition to the form. The email will be clear as to who is being approved or changed and the effective date and other details or reference so that the email and the form can be reconciled."

6. Unsupported Cost Allocation Percentages (New Finding)

OFM allocated $232,281 by strateg ic goals on the Statement of Net Costs based on unsupported cost allocation rates.

GAO *Standards for Internal Control for Federal Government* states that internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. All documentation and records should be properly managed and maintained.

Recommendation:

We recommend the OFM develop procedures for ensuring cost allocation rates used to prepare the Statement of Net Costs are properly supported and approved.

Management Response:

"The Director, OFM, made the unilateral decision to allow for some pre-existing allocation rates that pertain to older cost centers continue to be used for some remaining immaterial expenses. The Director, OFM will obtain the ET approval for these older cost center rates to be used until all expenses for all these cost centers are complete."

7. Lack of [redacted] Configuration Management Procedures (New Finding)

[redacted] does not have a documented process for configuration management. Only changes affecting additional systems are introduced as Configuration Control Board changes. Therefore, tracking of change approvals, successful testing, user acceptance testing, and supervisory approval for movement to production are not consistently documented.

Federal best practices noted in National Institute of Standards and Technology (NIST) SP800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*, control CM-1 states: "The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls." Additionally, control CM-3 states: "The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]]."

Recommendation:

We recommend the OHR develop and implement [redacted] configuration management process and procedures, including the tracking of change approvals, change testing, user acceptance testing, and supervisory approval for movement to production.

Management Response:

"USCP generally concurs with the finding. The Department will however adopt an alternate resolution option; the implementation of the existing OIS Change Management Policy and Procedures for any changes to the [redacted] System that can impact database information or compromise the integrity of payroll information. This will ensure a formal documented configuration management as it relates to [redacted]."

8. Lack of Vendor Support for Asset Management Application (New Finding)

USCP no longer has vendor support [redacted] for its asset management application, [redacted] On Sept 30, 2010, support for [redacted] and supporting components was withdrawn. This was announced on Sept 8, 2009 via [redacted]

USCP did not follow-up with [redacted] and sign-up for the two year annual extended service contract option which [redacted] made available to its clients that are unable to upgrade before September 30, 2010. To be eligible, clients must show that they are preparing an [redacted] upgrade roadmap. Extended service is priced at a premium and only available for two years.

USCP is responsible for maintaining vendor licenses and maintenance agreements for [redacted]. We noted through discussions with the Office of Financial Management System, that USCP is receiving support for database error through Library of Congress and CGI. USCP has a contract the Library of Congress to host the [redacted] application. However, USCP is responsible for all licensing, support and maintenance of [redacted]

Federal best practices noted in the *Federal Information Systems Controls Audit Manual* (FISCAM): Configuration Management (CM-5): Update software on a timely basis to protect against known vulnerabilities.

Patch Management: Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. A component of configuration management, it includes acquiring, testing, applying, and monitoring patches to a computer system. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. While most flaws do not create security vulnerabilities, the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.

National Institute of Standards and Technology (NIST) SP800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*, control SI-2 states: – "The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation.

Recommendation:

We recommend USCP upgrade [redacted] to a vendor supported version of the application.

Management Response:

"USCP has contracted with CGI Federal (CGI) to upgrade [redacted] from [redacted] to [redacted] is hosted by the Library of Congress who provides operational support. The project began September 30, 2011 and is expected to take approximately six months to fully implement, test and deploy. Currently the operational deployment date is identified as April 18, 2012.

CGI is providing overall project management and technical support for reviewing the existing system and relevant documentation, as well as providing gap analysis, planning, design, coordination, configuration management, development, test and implementation activities to support the [redacted] upgrade.

As of November 18, 2011, the following activities have been completed or are in progress:

1. draft schedule has been prepared (10/18)
2. coordination meeting with the LoC has been completed (11/9)
3. new hardware has been procured and delivered to the LoC (10/27)
4. the LoC environmental setup is being performed (complete by 12/7)
5. a test environment has been stood-up at CGI (11/17)
6. requirements analysis is being conducted (complete by 12/16)
7. a system test strategy is being developed (complete by 12/16)

Upon project completion [redacted] will be operational at the fully supported [redacted] and will have had all operational patches, security relevant patches, service packs and hot fixes applied, tested and documented."

9. Insufficient Oversight of External Information Systems (Prior Year Finding 3.16)

The USCP has not fully implemented controls to assess the external information systems. During fiscal year 2011, the Chief Information Security Officer began reviewing security documentation and assessments for the [redacted] Asset Management System supported by the Library of Congress Financial Hosting Environment. However, no review of the [redacted] security documentation and assessments had occurred during the fiscal year.

Federal best practices noted in the National *Institute of Standards and Technology (NIST) SP800-53 Revision 3 Recommended Security Controls for Federal Information*

Systems and Organizations, control SA-9 states – "The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers."

Recommendation:

We recommend the USCP document and implement review procedures for security documentation and assessments of external systems hosted at the Library of Congress Financial Hosting Environment.

Management Response:

"USCP has received the following security and Certification & Accreditation documents regarding [redacted] from the Library of Congress:

- Authority to Operate – dated 16 July 2011
- FIPS 199 Security Categorization – dated 14 April 2010
- 2011 3rd Quarter POA&M Report – dated 27 September 2011
- ST&E for [redacted] System – dated 2010
- Operational Risk Assessment – dated 15 July 2010
- Business Impact Analysis version 1.3 – dated 09 June 2010

The evidence will be reviewed by the USCP Chief Information Security Officer with a formal recommendation forwarded to the USCP CIO for final approval. The evidence will be reviewed to determine level of compliance, unaddressed associated risks, and completeness of operational impact, type and efficacy of security controls, tracking and reporting with POA&M utilization. The expected timeframe for completion of all review and reporting activities is January 31, 2012."