

**UNITED STATES CAPITOL POLICE  
FINANCIAL STATEMENTS AND  
INDEPENDENT AUDITORS' REPORT  
FISCAL YEAR 2006  
OIG-2007-04**

Cotton & Company LLP  
Auditors · Advisors  
635 Slaters Lane, 4<sup>th</sup> Floor  
Alexandria, Virginia 22314  
703.836.6701  
703.836.0941, fax  
[REDACTED]  
[www.cottoncpa.com](http://www.cottoncpa.com)

## CONTENTS

Section	Page
Independent Auditors' Report	1
Balance Sheet	2
Statement of Budgetary Resources	3
Notes to the Financial Statements	4
Independent Auditors' Report on Internal Control	9
Independent Auditors' Report on Compliance with Laws and Regulations	33



Cotton & Company LLP  
635 Slaters Lane  
4<sup>th</sup> Floor  
Alexandria, VA 22314

P: 703.836.6701  
F: 703.836.0941  
www.cottoncpa.com

United States Capitol Police Board

## INDEPENDENT AUDITORS' REPORT

We were engaged to audit the accompanying statement of financial position as of September 30, 2006 and the related statement of budgetary resources of the United States Capitol Police (USCP) for the year ended September 30, 2006. These financial statements are the responsibility of USCP management.

We were unable to form an opinion regarding the amounts at which property, plant and equipment, and accumulated depreciation are recorded in the accompanying statement of financial position at September 30, 2006 (stated at \$139,154,167 and \$57,908,775, respectively) because of the inadequacy of accounting records. We were unable to satisfy ourselves regarding the fair presentation of the fixed asset account balances by means of other auditing procedures.

Because we were unable to determine the amounts at which property, plant and equipment, and accumulated depreciation should be stated, and we were unable to apply other auditing procedures regarding the fair presentation of the fixed assets, as discussed in the preceding paragraph, the scope of our work was not sufficient to enable us to express, and we do not express, an opinion on the financial statements referred to in the first paragraph.

In accordance with *Government Auditing Standards*, we have submitted reports dated April 12, 2007, on USCP internal control over financial reporting and on compliance with provisions of laws and regulations. Those reports on internal control and compliance are an integral part of an audit conducted in accordance with *Government Auditing Standards*.

COTTON & COMPANY LLP

Alan Rosenthal, CPA  
Partner

April 12, 2007  
Alexandria, Virginia

**UNITED STATES CAPITOL POLICE  
BALANCE SHEET  
AS OF SEPTEMBER 30, 2006  
(IN DOLLARS)**

**ASSETS**

Intragovernmental:	
Fund Balance with Treasury (Note 2)	\$ 88,785,102
Advances to Others (Note 3)	3,825,550
Total Intragovernmental	92,610,651
Accounts Receivable, Net (Note 4)	46,562
General Property, Plant and Equipment, Net (Note 5)	<u>81,245,392</u>
<b>Total Assets</b>	<b><u>\$ 173,902,606</u></b>

**LIABILITIES (Note 6)**

Intragovernmental:	
Accounts Payable	\$ 5,346,494
Other (Note 7)	5,002,702
Total Intragovernmental	10,349,196
Accounts Payable	6,555,956
Unfunded Actuarial Workers' Compensation Benefits	20,022,294
Other (Note 7)	<u>15,094,861</u>
<b>Total Liabilities</b>	<b><u>52,022,306</u></b>

**NET POSITION**

Unexpended Appropriations	70,255,739
Cumulative Results of Operations	<u>51,624,560</u>
<b>Total Net Position</b>	<b><u>121,880,299</u></b>

<b>Total Liabilities and Net Position</b>	<b><u>\$ 173,902,606</u></b>
---	------------------------------

The accompanying notes are an integral part of this financial statement.

**UNITED STATES CAPITOL POLICE  
STATEMENT OF BUDGETARY RESOURCES  
FOR THE YEAR ENDED SEPTEMBER 30, 2006  
(IN DOLLARS)**

**Budgetary Resources**

Unobligated balance, brought forward, October 1	\$ 47,080,936
Recoveries of prior-year unpaid obligations	10,800,847
Budget authority:	
Appropriation	249,456,000
Spending authority from offsetting collections	1,076,853
Nonexpenditure transfers, net	-
Permanently not available	<u>(2,494,560)</u>
<b>Total Budgetary Resources</b>	<b><u>\$ 305,920,076</u></b>

**Status of Budgetary Resources**

Obligations incurred:	
Direct	
Exempt from apportionment	\$ 265,913,061
Unobligated balance:	
Exempt from apportionment	33,885,625
Unobligated balance not available	<u>6,121,390</u>
<b>Total Status of Budgetary Resources</b>	<b><u>\$ 305,920,076</u></b>

**Change in Obligated Balance**

Obligated balance, net	\$ 50,469,289
Obligations incurred, net	265,913,061
Less: Gross Outlays	256,854,853
Less: Recoveries of prior year unpaid obligations, actual	<u>10,800,847</u>
<b>Obligated balance, net, end of period</b>	<b><u>\$ 48,726,650</u></b>

**Net Outlays**

Gross Outlays	\$ 256,854,853
Less: Offsetting collections	1,076,853
Less: Distributed Offsetting receipts	<u>0</u>
<b>Net Outlays</b>	<b><u>\$ 255,778,001</u></b>

The accompanying notes are an integral part of this financial statement.

**UNITED STATES CAPITOL POLICE  
NOTES TO THE FINANCIAL STATEMENTS  
FOR THE YEAR ENDED SEPTEMBER 30, 2006**

**NOTE 1.        SIGNIFICANT ACCOUNTING POLICIES**

**Reporting Entity**

The accompanying financial statements present the financial position and budgetary resources of the United States Capitol Police (USCP). The mission of the USCP, an agency in the legislative branch of the federal government, is "to protect the Congress, its legislative processes, Members, employees, visitors, and facilities from crime, disruption, or terrorism." The USCP carries out its mission primarily by providing security for the Capitol and congressional office buildings, protective services for Members and dignitaries, installing and operating advanced security systems, and maintaining staff and equipment to provide emergency response within its jurisdiction.

**Basis of Accounting**

The USCP's financial statements, consisting of a balance sheet and a statement of budgetary resources as of and for the fiscal year ended September 30, 2006 have been prepared in conformity with accounting principles generally accepted in the United States of America as applicable for the federal government and have also been prepared in accordance with guidance prescribed in Office of Management and Budget (OMB) Circular A-136, *Financial Reporting Requirements*. OMB A-136 constitutes generally accepted accounting principles for the federal government as specified by the AICPA's Statement on Auditing Standards (SAS) 69, as amended, *The Meaning of Presents Fairly in Conformity with Generally Accepted Accounting Principles*.

**Assets**

Intra-governmental assets are those assets that arise from transactions with other Federal entities. Funds with the U.S. Treasury comprise the majority of intra-governmental assets on USCP's balance sheet.

**Fund Balance with Treasury**

The U.S. Treasury processes USCP's receipts and disbursements. Funds with the U.S. Treasury primarily represent appropriated funds that are available to pay current liabilities and finance authorized purchase commitments. See Note 2 for additional information.

**Advances and Prepayments**

The USCP advances funds to federal agencies to perform long-term capital projects. The advances are liquidated and recorded as expenses or capitalized assets, as work is completed.

**General Property, Plant and Equipment**

General Property, Plant, and Equipment (PP&E) consists of equipment, structures, facilities, building improvements, internal use software, and construction-in-progress. The basis for recording purchased PP&E is full cost, which includes all costs incurred to bring the PP&E to a form and location suitable for its intended use. The USCP purchases assets directly from or via contracts with commercial vendors, and through interagency agreements with other federal agencies. Assets costing more than \$25,000 are capitalized and depreciated on a straight-line basis over the estimated useful life of the property as

follows: computer hardware and software, 3 years; equipment and motor vehicles, 5 years; trucks and vans, 7 years; building improvements, other structures and facilities, 10 years.

### **Liabilities**

Liabilities represent amounts that are likely to be paid by the USCP as a result of transactions or events that have already occurred.

### **Accounts Payable**

Accounts payable consists of amounts owed to other federal agencies and commercial vendors for goods and services received and accepted prior to the end of the reporting period.

### **Federal Employee Benefits**

USCP recognizes its share of the cost of providing future pension benefits to eligible employees over the period of time that they render services to USCP. The pension expense recognized in the financial statements equals the current service costs for USCP's employees less the amount contributed by the employees. OPM, the administrator of the plan, supplies USCP with the factors to apply in the calculation of the service cost. These factors are derived through actuarial cost methods and assumptions. The excess of the recognized pension expense over the amount contributed by USCP and employees represents the amount being financed directly through the Civil Service Retirement and Disability and administered by OPM. This amount is considered imputed financing to USCP.

FECA provides income and medical cost protection to covered federal employees injured on the job, employees who have incurred a work-related occupational disease, and beneficiaries of employees whose death is attributable to a job-related injury or occupational disease. Claims incurred for benefits for USCP employees under FECA are administered by the Department of Labor (Labor) and are paid, ultimately by USCP.

USCP recognizes a current-period expense for the future cost of postretirement health benefits and life insurance for its employees while they are still working. USCP accounts for and reports this expense in its financial statements in a manner similar to that used for pensions, with the exception that employees and USCP do not make current contributions to fund these future benefits.

### **Annual, Sick, and Other Leave**

Annual leave is accrued as it is earned and the accrual is reduced as leave is taken. Each year, the balance in the accrued leave account is adjusted to reflect current pay rates and balances. To the extent current or prior year appropriations are not available to fund annual leave earned but not taken, funding will be obtained from future financing sources. Sick leave and other types of non-vested leave are expensed as taken. All leave is funded when expensed.

### **Contingencies**

There are no commitments or contingencies that require disclosure.

### **Estimates**

Management has made certain estimates and assumptions when reporting assets, liabilities, revenue and expenses, and in the note disclosures. Actual results could differ from these estimates.

**NOTE 2. FUND BALANCE WITH TREASURY**

Fund Balances with Treasury are the aggregate amounts of the USCP's accounts with Treasury for which the entity is authorized to make expenditures and pay liabilities. The Memorial Fund includes amounts donated to the United States Capitol Police Memorial Fund. Some of these funds are restricted for intended purposes.

<u>Fund Type</u>	<u>Balance</u>
Appropriated	\$88,733,665
Special (Memorial Fund)	33,435
Suspense	9,155
Miscellaneous Receipt	8,847
Total	<u>\$88,785,102</u>

**Status of Appropriated Balance**

Unobligated	
Available	\$33,885,625
Unavailable	6,121,390
Obligated Balance not yet Disbursed	<u>48,726,650</u>
Total	<u>\$88,733,665</u>

**NOTE 3. ADVANCES TO OTHERS**

The USCP enters into agreements with other federal agencies to design, develop, and test security systems. These agencies estimate funding necessary for payments to their contractors for labor and materials for certain periods of time and request advances of funds from USCP. The advances are periodically liquidated using information from expense reports sent to USCP. Any unliquidated advance balance remaining at the end of the project is refunded to USCP by the agencies holding the contract.

**NOTE 4. ACCOUNTS RECEIVABLE**

Receivables from the public:	
Commercial vendors	\$ 1,124
USCP Employees	66,817
Allowance for uncollectible accounts	(21,379)
Net Receivables	\$46,562

The allowance for uncollectible accounts is calculated by the National Finance Center (NFC) and pertains to receivables due from USCP employees. The calculation is based on a risk of non-collection factor applied to an aging of the receivables.

<u>Days Outstanding</u>	<u>Factor</u>	<u>Receivable</u>	<u>Allowance</u>
0-90 days	.01	\$34,697	\$ 595
91-180 days	.25	286	72
181-360 days	.50	9,495	4,747
Over 360 days	.90	20,583	15,965
Total			<u>\$21,379</u>



**NOTE 5. PROPERTY, PLANT, AND EQUIPMENT**

The composition of property, plant and equipment as of September 30, 2006, is as follows:

<b>Classification</b>	<b>Acquisition Cost</b>	<b>Accumulated Depreciation</b>	<b>Book Value</b>
Building Improvements	\$ 609,090	\$ 145,788	\$ 463,302
Other Structures and Facilities	1,444,667	466,922	977,745
Equipment	74,186,306	54,061,438	20,124,868
Internal Use Software	7,293,101	3,234,626	4,058,475
Construction-In-Process	55,419,624	- 0 -	55,419,624
Software-In-Development	201,379	- 0 -	201,379
<b>Total</b>	<b><u>\$139,154,167</u></b>	<b><u>\$57,908,774</u></b>	<b><u>\$81,245,393</u></b>

**NOTE 6. LIABILITIES NOT COVERED BY BUDGETARY RESOURCES**

USCP liabilities not covered by budgetary resources as of September 30, 2006 are summarized below:

<b>Intragovernmental</b>	
Other: Accrued Unfunded FECA	\$ 2,069,615
<b>Workers' Compensation Benefits (Actuarial FECA Liability)</b>	20,022,294
Other: Accrued Unfunded Leave	<u>7,869,075</u>
<b>Total Liabilities Not Covered by Budgetary Resources</b>	<b><u>\$29,960,984</u></b>

The actuarial liability for future workers' compensation benefits includes the expected liability for death, disability, medical, and miscellaneous costs for approved compensation cases, plus a component for incurred but not reported claims. The liability utilizes historical benefit payment patterns related to a specific incurred period to predict the ultimate payment related to that period. Liabilities not covered by budgetary resources require Congressional action before budgetary resources can be provided. Although future appropriations to fund these liabilities are likely, it is not certain such appropriations will be enacted.

**NOTE 7. OTHER LIABILITIES**

<b>Intragovernmental</b>	
Accrued Unfunded FECA Liability	\$2,069,615
Accrued Funded FECA Liability	<u>2,933,087</u>
Total	\$5,002,702
<b>Non-Federal</b>	
Accrued Funded Payroll and Leave	7,171,504
Unfunded Annual Leave	7,869,075
Funds Returned by Treasury, Canceled Payments to be Reissued	12,000
Custodial Receipts Held for Others	<u>42,282</u>
Total	<u>\$15,094,861</u>
<b>Total Other Liabilities</b>	<b><u>\$20,097,563</u></b>

**NOTE 8. FEDERAL EMPLOYEE BENEFITS**

All permanent employees participate in the contributory Civil Service Retirement System (CSRS) or the Federal Employees Retirement System (FERS). Temporary employees and employees participating in FERS are covered under the Federal Insurance Contributions Act (FICA). To the extent that employees are covered by FICA, the taxes they pay to the program and the benefits they will eventually receive are not recognized in USCP's financial statements. USCP makes contributions to CSRS, FERS, and FICA and matches certain employee contributions to the thrift savings component of FERS. All of these payments are recognized as operating expenses.

In addition, all permanent employees are eligible to participate in the contributory Federal Employees Health Benefit Program (FEHBP) and Federal Employees Group Life Insurance Program (FEGLIP) and may continue to participate after retirement. USCP makes contributions through OPM to FEHBP and FEGLIP for active employees to pay for their current benefits. USCP's contributions for active employees are recognized as operating expenses. Using the cost factors supplied by OPM, USCP has also recognized an expense in its financial statements for the estimated future cost of postretirement health benefits, retirement, and life insurance for its employees. These costs are financed by OPM and imputed to USCP.

Amounts owed to OPM and Treasury as of September 30, 2006, are \$1,213,646 for FEHBP, FEGLIP, FICA, FERS, and CSRS contributions and are shown on the Balance Sheet as payroll liabilities. Details of the major components of USCP's federal employee benefit costs for the year ended September 30, 2006, are as follows:

Pension expenses, including Thrift Savings Plan (CSRS/FERS)	\$39,373,619
Health and life insurance expenses (FEHBP/FEGLIP)	\$19,943,481
FICA payment, including Medicare, made by USCP	\$19,943,164
Federal employee retirement benefit costs paid by OPM and imputed to USCP:	
Estimated future pension costs (CSRS/FERS)	\$ 6,670,772
Est. future post-retirement health and life insurance (FEHBP/FEGLIP)	\$ 9,016,113

**NOTE 9. INCIDENTAL CUSTODIAL COLLECTIONS**USCP Memorial Fund (Treasury Symbol 02X5083)

Beginning Balance (as of October 1, 2005)	\$48,686
Donations Collected and Deposited to the U.S. Treasury	43,485
Disbursements to Recipients	(58,736)
Ending Balance (as of September 30, 2006)	<u>\$33,435</u>

**NOTE 10. WORKERS' COMPENSATION**

The USCP recorded an estimated liability for claims incurred but not reported as of September 30, 2006, which is expected to be paid in future periods. This estimated liability of \$20,022,294 is reported on USCP's Balance Sheet. The USCP also recorded a liability for amounts paid to claimants by the Department of Labor but not yet reimbursed by USCP in the amount of \$5,002,702 and is shown in USCP's Balance Sheet as an intragovernmental liability.



Cotton & Company LLP  
635 Slaters Lane  
4<sup>th</sup> Floor  
Alexandria, VA 22314

P: 703.836.6701  
F: 703.836.0941  
www.cottoncpa.com

United States Capitol Police Board

## INDEPENDENT AUDITORS' REPORT ON INTERNAL CONTROL

We have examined the effectiveness of the United States Capitol Police (USCP) internal control over financial reporting as of September 30, 2006, based on the *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States. USCP management is responsible for maintaining effective internal control over financial reporting. Our responsibility is to express an opinion on effectiveness of internal control based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and *Government Auditing Standards*, issued by the Comptroller General of the United States. Thus, our examination included obtaining an understanding of internal control over financial reporting, testing and evaluating the design and operating effectiveness of internal control, and performing such other procedures we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in any internal control, misstatements due to error or fraud may occur and may not be detected. Also, projections of any evaluation of the internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with policies or procedures may deteriorate.

During Fiscal Year (FY) 2006, two reportable conditions were identified, which are considered material weaknesses. USCP lacked policies and procedures to ensure that payroll activity was processed consistently and adequately supported. In addition, USCP had incomplete financial management policies, methods, and procedures that did not ensure complete, accurate, and timely reporting of financial information.

A material weakness is a condition that precludes USCP's internal control from providing reasonable assurance that material misstatements in the financial statements will be prevented or detected on a timely basis. We provide details on these material weaknesses (Findings No. 1 and 2) in an attachment to this report.

We also noted one reportable condition identified during the examination (Finding No. 3) that we do not consider to be a material weakness. USCP had incomplete information system controls that did not ensure complete, accurate, and timely reporting of financial information. We consider this matter to be a reportable condition. A reportable condition is a matter that comes to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect an agency's ability to record, process, summarize, and report financial data consistent with management assertions in the financial statements.

In our opinion, because of the effects of the material weaknesses described in the fourth paragraph on achieving objectives of the control criteria, USCP had not maintained effective internal control over financial reporting as of September 30, 2006, based on *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

~~This report is intended solely for the information for and use of United States Capitol Police Board, USCP management, Members of the United States Congress, and the Comptroller General of the United States and is not intended to be, and should not be, used by anyone other than these specified parties.~~

COTTON & COMPANY LLP



Alan Rosenthal, CPA  
Partner

April 12, 2007  
Alexandria, Virginia

**UNITED STATES CAPITOL POLICE  
REPORT ON INTERNAL CONTROL WEAKNESSES  
FISCAL YEAR 2006 FINANCIAL STATEMENT AUDIT**

In performing the Fiscal Year (FY) 2006 financial statement audit of the United States Capitol Police (USCP), the audit identified three reportable conditions. Two of these are considered to be material weaknesses. These findings are reported here.

These three conditions were also reported in the FY 2005 audit report. USCP has made some progress toward implementing recommendations. The material weakness associated with payroll processing still, however, exists, and the prior year reportable condition associated with Financial Management is elevated to a material weakness. Therefore, we recommend that the Chief Administrative Officer (CAO) continue actions to implement prior recommendations, as well as any new recommendations described herein.

This document begins with a list of criteria we applied to internal control weaknesses and concludes with details about specific weaknesses we identified.

**CRITERIA**

We used three levels of progress to rank improvement of prior findings:

- Substantial Progress
- Some Progress
- Limited Progress

We based the status of prior recommendations on the following criteria:

- Closed
- Substantial Progress
- Some Progress
- Limited Progress
- Not Started

## DETAILS OF INTERNAL CONTROL WEAKNESSES

### Finding No. 1: Payroll Processing

**Summary Status:**   Material Weakness  
                          Prior Condition  
                          Some Progress

NFC processes payroll for USCP. USCP must report time and attendance to NFC and is responsible for maintaining pay and leave records and documents that support pay rates and deductions. USCP lacked policies and procedures to ensure that payroll and personnel activity for which it was responsible was processed consistently and properly supported by approved and authorized documentation.

This condition has been reported since FY 1999, and similar elements of the condition existed as of September 30, 2006. Prior-year audits and the FY 2006 audit identified eight conditions that resulted in this material weakness. The recommendations for each of these conditions are still open and are discussed below.

**1. USCP employee personnel folders did not contain documents to support various payroll actions, and documents found did not agree to current payroll actions reported. Documentation was not always present to support current employee salaries.**

We recommend that the CAO develop and implement policies and procedures to ensure that employee personnel files are current and clearly document grade, step, and benefit information for each employee, and that supporting documentation for all payroll disbursements is readily available.

#### **Status of Recommendation: Substantial Progress.**

USCP has developed procedures to ensure that current salary information is appropriately reflected in the personnel records and that individual payroll data are properly controlled, supported, and maintained. Specific personnel are in place to perform the developed procedures.

**Open:** USCP needs to implement an additional level of quality assurance to ensure proper maintenance of all personnel records.

#### **Management Response:**

Beginning in January of 2005, USCP adopted the use of Form SF-50, "Notification of Personnel Action," and printed hard-copy documents for inclusion in the Department's Central Personnel Files. Prior to that date, all records of payroll data were captured in the human resources information system. Extensive work has been completed to ensure that adequate documentation capturing employees' grade, step and benefit information is filed to support payroll disbursements. OHR staff, who have been performing these procedures for over a year, are currently conducting an audit of each record to ensure compliance, as well as developing written standard operating procedures scheduled to be completed by September 30, 2007.

It is important to note, that the data tested during this audit supported the significant efforts of the staff to ensure compliance. 45 employee records were tested in which 96% of the records passed signing and filing requirements. This is a remarkable

	achievement in a very short time frame, considering one-year prior; no records had been signed or contained filed SF-50's. USCP believes that the variance of 4% is within a reasonable acceptance level for compliance, and merits consideration to close this recommendation.
--	---

**2. USCP policy requiring all employees to positively attest to the accuracy of pay-period information transmitted to NFC is not consistently implemented.**

We recommend that the CAO develop and implement policies and procedures requiring all employees to positively attest to the accuracy of pay-period information transmitted to NFC.

**Status of Recommendation: Limited Progress.**

USCP has developed procedures requiring employees to acknowledge their review of the bi-weekly Certification Report to the extent practical. Employees are required to sign and date reports and to promptly disclose discrepancies to supervisors. Implementation of the procedure remains inconsistent. USCP has implemented a new time collection system that could render the acknowledgement of the Certification Report obsolete; the control function has not been activated. The primary policy directing this issue currently is the requirement for each employee to sign the Certification Report.

An additional control to mitigate this condition was implemented just prior to the audit beginning in January 2007. This control consisted of timekeepers sending an email to OHR to inform OHR of the execution of Certification Directive. While this control was not in place during the fiscal year under audit it was evaluated and found to be not effective. During testing of positive confirmation emails, it was found that the emails were not accurate representations of the execution of the policy. In order for this new control to be effective additional staff training and supervisory follow up is needed.

**Open:** USCP needs to implement and enforce policies and procedures. If USCP intends to use the controls built into the new time collection system to correct this condition, its policies must be updated to reflect which policy is in effect and required. If the USCP is to continue its current procedures they must evaluate the certification procedures on a

**Management Response:**

As a result of prior year audit recommendations, OHR published Special Directive [REDACTED] in late December of 2006. USCP auditors tested the sample of several offices one-pay period after implementation and did not find 100% compliance. USCP/OHR recognizes that a change in procedures can be cumbersome and confusing and therefore conducted one-on-one training with several timekeepers. In addition, OHR will be testing offices throughout the summer to ensure compliance with an expectation for improved results.

A second level of assurance was put in place requiring senior level managers to report their offices' compliance with the requirement to certify time and attendance. A report is generated each pay period listing the offices that comply and those that fall short. Attention has been devoted to this requirement at the highest levels of the department and is part of the internal control process for payroll processing.

Upcoming research and planning efforts will focus on automating the supervisory certification process in the Time and Attendance system during the summer. Guidance documents provided by GAO indicate that the USCP has required a greater threshold for employee certification than is required government-wide. Specifically, in its January 2003 Internal Control Report on

consistent basis to ensure 100% compliance.	<p>"Maintaining Effective Control over Employee Time and Attendance Reporting", GAO provides discretion on the employee attestation of time and attendance records in both manual and electronic environment. USCP will focus on 100% compliance by supervisors, keeping employees informed of their work hours during each pay period. Risk for 100% compliance prior to payroll processing may result in some employees not receiving their payroll disbursements in a timely fashion. OHR will work to address new procedures for meeting this finding.</p>
---	--

<p><b>3. USCP did not enforce its policy requiring supervisors to approve the accuracy of pay-period information submitted to NFC.</b></p> <p>We recommend that the CAO enforce existing policies and procedures to require supervisors to approve the accuracy of pay-period information transmitted to NFC.</p>	
<p><b>Status of Recommendation: Limited Progress.</b></p> <p>USCP has developed procedures requiring supervisors or other equivalent officials most knowledgeable of time worked by employees to approve bi-weekly Certification Reports to the extent practical. They are required to sign and date reports; however, inconsistent application has been noted. USCP has implemented a new time collection system that could render the acknowledgement of the Certification Report obsolete. This control function has not been activated. An additional control to mitigate this condition was implemented just prior to the audit beginning in January 2007. This control consisted of timekeepers sending an email to OHR to inform OHR of the execution of Certification Directive. While this control was not in place during the fiscal year under audit it was evaluated and found to be not effective.</p> <p><b>Open:</b> USCP needs to consistently implement policies and procedures. If USCP intends to use the controls built into the new time collection system to correct this condition, it must update current policies and notify all personnel of the change.</p>	<p><b>Management Response:</b></p> <p>As a result of prior year audit recommendations, OHR published Special Directive [REDACTED] in late December of 2006. USCP auditors tested the sample of several offices one-pay period after implementation and did not find 100% compliance. USCP/OHR recognizes that a change in procedures can be cumbersome and confusing and therefore conducted one-on-one training with several timekeepers. In addition, OHR will be testing offices throughout the summer to ensure compliance with an expectation for improved results.</p> <p>A second level of assurance was put in place requiring senior level managers to report their offices' compliance with the requirement to certify time and attendance. A report is generated each pay period listing the offices that comply and those that fall short. Attention has been devoted to this requirement at the highest levels of the department and is part of the internal control process for payroll processing.</p> <p>Upcoming research and planning efforts will focus on automating the supervisory certification process in the Time and</p>



	<p>Attendance system during the summer. Guidance documents provided by GAO indicate that the USCP has required a greater threshold for employee certification than is required government-wide. Specifically, in its January 2003 Internal Control Report on "Maintaining Effective Control over Employee Time and Attendance Reporting", GAO provides discretion on the employee attestation of time and attendance records in both manual and electronic environment. USCP will focus on 100% compliance by supervisors, keeping employees informed of their work hours during each pay period. Risk for 100% compliance prior to payroll processing may result in some employees not receiving their payroll disbursements in a timely fashion. OHR will work to address new procedures for meeting this finding.</p>
--	--

<p><b>4. USCP did not maintain adequate timekeeping records. Signed Certification Reports could not be located. Without signed Certification Reports, it is not possible to verify that information in the time collection system is authorized and accurate.</b></p> <p>We recommend that the CAO develop and implement policies and procedures to permit USCP to efficiently track and certify all hours incurred by all employees.</p>	
<p><b>Status of Recommendation: Some Progress.</b></p> <p>The Certification Report is intended to be the primary control for time attestation, these documents must be retained. Any changes or adjustments must be documented. The new system requires the T&amp;A Clerk to enter an explanation into the system to document changes. Supervisory attestation, however, did not always occur.</p> <p><b>Open:</b> USCP needs to ensure that all time is attested to before this deficiency can be considered closed. Additionally, changes to timekeeping records made directly to the time collection system should require re-certification of Certification Reports. Completed Certification Reports should be kept in a central location and controls put in place to ensure that all reports are maintained.</p>	<p><b>Management Response:</b></p> <p>Upcoming research and planning efforts will focus on automating the supervisory certification process in the Time and Attendance system during the summer. Guidance documents provided by GAO indicate that the USCP has required a greater threshold for employee certification than is required government-wide. Specifically, in its January 2003 Internal Control Report on "Maintaining Effective Control over Employee Time and Attendance Reporting", GAO provides discretion on the employee attestation of time and attendance records in both manual and electronic environment. USCP will focus on 100% compliance by supervisors, keeping employees informed of their work hours during each pay period. Risk for 100% compliance prior to payroll processing may result in some employees not receiving their payroll disbursements in a timely fashion. OHR will work to address new procedures for meeting this finding.</p>

	OHR will work to address new procedures for meeting this finding which will eliminate the hardcopy certification report and require the supervisory certification of changes to previously transmitted time and attendance records. This change in work procedure will be addressed by September 30, 2007.
--	--

**5. Controls to provide evidence of approval of overtime and leave in [REDACTED] or the certification report were not consistently used.**

We recommend that the CAO enforce policies and procedures regarding supervisory approval of time records and reinforce policies and procedures regarding leave approval.

**Status of Recommendation: Limited Progress.**

The requirement for overtime and leave approval in [REDACTED] was not made into a formal USCP Directive. The only approval required is on the certification report.

**Management Response:**

USCP has policies and procedures addressing the authorization and approval for overtime for both non-exempt and exempt employees. Procedure guidance to managers and supervisors was distributed in 2005 and 2006, which will be formalized in an Additional Duty Directive scheduled to be published by February 2008.

Procedures for scheduling and approving leave exist, and all employees are required to use Form [REDACTED]. Auditors tested the operational procedures of several timekeepers and found one timekeeper who did not follow proper procedures. This is not a failure of the Department's policies, but rather identifies opportunities where training and supervisory oversight are needed in that particular Division.

USCP anticipates the publication of new leave policy and procedures by February 2008. OHR personnel have revamped all 25 outdated policies and written a comprehensive document covering all categories of leave and the procedures for its use.

<b>6. Physical security of personnel records and personnel related information was inadequate.</b>  We recommend that the CAO develop policies and procedures to properly safeguard sensitive information related to personnel to prevent unauthorized access and loss and implement them.	
<b>Status of Recommendation: Closed.</b>	<b>Management Response:</b>  USCP management concurs with this closure.

<b>7. a.) Office of Human Resources (OHR) did not perform a detailed reconciliation of payroll data before and after transmission to NFC. (B3007)</b>  <b>b.) Additionally, OHR did not review the Audit Report titled "Review of the Office of the Chief Financial Officer/National Finance Center General Controls" (SAS 70). This report identifies weaknesses in NFC internal controls that should be considered when controls are designed and evaluated by USCP.</b>  We recommend that the CAO develop policies and procedures to regularly perform a robust reconciliation of all data transmitted to and received from NFC to verify its integrity. Additionally, we recommend the CAO develop policies and procedures to regularly obtain the SAS 70 report from NFC and document an evaluation of the potential impact that NFC weaknesses can have on USCP.	
<b>Status of Recommendation:</b>  <b>a.) Some Progress.</b>  USCP recognizes the need for a detailed reconciliation. Meetings were held to discuss the scope of the reconciliation needed.  <b>b.) Closed.</b>	<b>Management Response:</b>  a) For every pay period, USCP/OHR personnel reconcile the number of time and attendance records transmitted to NFC with the number of time and attendance records received by NFC for payroll purposes. During prior audits, USCP did not have the benefit of understanding exactly what the auditors meant by a "detailed" reconciliation of the time and attendance data. As a result of work efforts during this year's audit, OHR managers requested to meet with auditors to clearly define the expectation and to gain a common understanding of the difference between time and attendance data (hours transmitted) versus payroll data (dollars paid). This common understanding resulted in OHR accessing the OFM payroll files and programming compliance reports to compare the hours transmitted against the hours/dollars paid to ensure that either no changes occurred to an employee's records or that any changes could be documented and legitimately verified.  Designated OHR personnel receive a bursted email report every payroll week comparing the transmitted data with the received payroll data. By September 30, 2007, published procedures will be developed to support the reconciliation and

	<p>subsequent resolution process performed each week.</p> <p>b) USCP management concurs with this closure.</p>
--	--

**8. OHR did not have sufficient controls in place to ensure compliance with Federal Nepotism Laws and Regulations.**

We recommend that the CAO develop policies and procedures to prevent non-compliance with Title 5, Part III of Section 3110, Employment of relatives; restrictions. Multiple levels of control may be needed to guarantee that the law will not be violated.

**Status of Recommendation: Substantial Progress.**

USCP has several policies related to the employment of relatives, additionally a specific policy "Employment of Relatives" has been drafted and is currently under review by USCP management officials. However, once hired, monitoring to maintain compliance is not consistent. Automated procedures are being developed to assist USCP personnel comply with this regulation when transfers or temporary duty assignments occur. USCP should continue developing the automated systems to assist the monitoring of this regulation.

**Management Response:**

Since the inception of the "nepotism" policy, USCP has collected and stored applicable data in the [REDACTED] system. Further, the Background Investigation Booklet for Law Enforcement has been automated in the [REDACTED] staffing system, which will capture information on nepotism. The process is currently under a pilot study to address operating bugs within the system. The projected implementation is scheduled in the fall 2007.

Similarly, the Background Investigation Booklet for civilians is currently under review for automation, and it too will capture and store relevant information on employment of relatives. The automated Booklets will cover the entire Department, and both the [REDACTED] and [REDACTED] systems will have the capacity to generate appropriate reports, as required. The nepotism policy for processing personnel actions includes entry-level positions, detail assignments, promotions, transfers and special assignments.

The [REDACTED] system will be able to identify any matches with relatives on both sides of a personnel action and will generate a report. HR will then investigate the match for quality assurance before any personnel action is initiated. This will be completed by September 30, 2007.

<p><b>9. OHR did not have controls in place to ensure compliance with the objectives of the USCP Student Loan Repayment Program.</b></p> <p>We recommend that the CAO develop detailed procedures to guide employees and supervisors responsible for the implementation of the program. Additionally, performance metrics must be defined in order to measure the success of the program. The USCP Office of Inspector General is issuing an additional report on this subject.</p>	
<p><b>Status of Recommendation: Not Started.</b></p>	<p><b>Management Response:</b></p> <p>During the spring of 2007, in anticipation of the OIG report, OHR personnel have completed the following action items to address the lack of oversight and procedures for the Student Loan Repayment Program (SLRP) administration. Specifically, the following tasks have been accomplished:</p> <ul style="list-style-type: none"> <li>• Creation of new forms and Standard Operating Procedure for the SLRP.</li> <li>• Requirement that applicants in the SLRP authorize direct account access to USCP OHR representative.</li> <li>• Addition of SLRP to OHR separation checklist.</li> <li>• Implementation of a process whereby the OHR Employee Relations (ER) Section receives a separation report each pay period to cross check SLRP participants with separation to determine the necessity for recoup of benefits.</li> <li>• Creation of applicant checklist to ensure paperwork is filed appropriately.</li> <li>• Securement of additional storage space for SLRP files.</li> <li>• Creation of a standard reporting format for annual reporting.</li> </ul> <p>OHR anticipates continual improvements to the program and will diligently work to more effectively manage this key human capital tool for the Department.</p>

## **Finding No. 2: Financial Management**

**Summary Status:**   Material Weakness  
                              Prior Condition  
                              Some Progress

The prior-year internal control examination disclosed that USCP had inadequate and incomplete accounting policies, methods, practices, and systems, which contributed to poor financial management. USCP has continued to make improvements since FY 1999. Although our FY 2006 examination found that this condition continued to exist as of September 30, 2006, new weaknesses were identified as a result of new challenges that arose. During FY 2004, FY 2005, and into FY 2006, USCP implemented many recommended policies and procedures; however, severe loss of human capital resources had a significant impact on USCP's financial reporting capability. The environment surrounding USCP financial management continues to evolve as evidenced this year by the implementation of a new accounting system. USCP prepared a statement of budgetary resources for a third year and also prepared a balance sheet for the first time. The combination of staff shortages, a new accounting system, and the first year balance sheet preparation taxed USCP Office of Financial Management (OFM) beyond their capacity. The conditions created by these elements resulted in a reportable condition considered to be a material weakness. At the time of this report USCP is taking positive steps to react to these conditions, however, they continue to face challenges and difficulties with daily operations caused by growth and staff shortages. Several key positions that had been vacant have been recently filled with new personnel. The OFM will have difficulties responding to recommendations until the new staff has been fully and adequately trained.

### **1. OFM did not fully implement and monitor policies and procedures for managing financial operations.**

As of September 30, 2006, OFM had developed and implemented policies and procedures for managing financial operations, but they were not consistently applied because of the lack of manpower. The most important aspect of implementing new policies is following up on how well staff is employing the new procedures. Unless new and current policies and procedures are clearly presented by management and understood and followed by all employees, USCP will continue to have deficiencies in financial operations.

Specifically, we noted the following deficiencies:

- Misclassified transactions (Budget Object Codes) (C4002)
- Vendors not promptly paid (although not required by law) (C3006)
- Payment documentation not thoroughly reviewed (C4001)
- No policy or procedure requiring the monitoring of fuel purchase transactions (C3002)
- Purchase card and Travel card differences reported on the SF-6652 were not resolved in a timely manner. (A3001), (A4006)
- Evidence of supervisory review of cash reconciliations was not present. (A3002)
- Monthly Payroll reconciliations were not completed in a timely fashion. (B3013),

(B3010)

We recommend that the CAO continue to monitor implementation of policies and procedures covering all matters impacting USCP's financial performance, take steps to provide available staff to ensure that policies and procedures are implemented consistently throughout USCP, and provide training for all employees.

**Status of Recommendation: Some Progress.**

USCP developed a Financial Management Improvement Plan (FMIP) in FY 2001 that included policies and procedures for operating OFM and HRM. It has implemented many policies and procedures, but follow-up must occur to ensure that they are consistently followed. Additionally, policies and procedures should be developed for all activities occurring in OFM. Severe staffing shortages created a condition in which in some cases there was no personnel to perform the procedures for which policies had been written. USCP began working on an internal control evaluation program similar to A-123; however work was temporarily suspended due to lack of manpower.

**Open:** USCP needs to continue development of its internal control evaluation program. Additionally, USCP needs to monitor its manpower more closely to prevent such a severe shortage from occurring again.

**Management Response:**

USCP continues to develop a comprehensive set of financial management policies and procedures. To facilitate this development and ensure all major processes are properly documented. The Department has procured contractual support services to perform an internal controls assessment in accordance with OMB A-123 Appendix A, *Management's Responsibility for Internal Control over Financial Reporting*. This analysis will look at the USCP control environment, and utilize a top-down approach to planning, testing and documenting internal controls and associated policies and procedures over financial reporting encompassing significant agency-wide financial reports and working back to the key processes, controls and supporting documentation. This initial documentation and assessment effort is expected to be completed in October 2007.

USCP has allocated two additional resources in the Office of Financial Management, one each to the Budget and Accounting Divisions and has requested four additional positions in the fiscal year 2008 budget request.

USCP immediately advertises and/or backfills positions when employee turnover occurs and works closely between OFM and OHR to fill positions as quickly as possible based on the current hiring process.

**2. OFM had inadequate quality assurance procedures for yearend closing and financial statement preparation.**

OFM continues to struggle with producing the fiscal yearend financial statements. While most of the difficulty arose from the conversion of the old accounting system to the new system, additional issues were caused by the change in statement format and inexperienced staff. OFM prepared its first statement of financial position in FY 2006. As stated previously, difficulties arose due to inexperience.

Specifically, we noted the following deficiencies:

- Policies and procedures for providing evidence of supervisory review of the Financial Statements before submission to end users were not followed. (A3004)
- Controls to ensure proper closure of yearend accounts were lacking. (A4001, A4002)
- USCP's SBR line item, Net Outlay, did not agree to Treasury-reported GWA, Government-Wide Accounting Balance. (A4010)
- OFM did not record payables when goods and services were received and lacked a substantive methodology to estimate a sufficient liability. (C3001) (C4003)
- OFM did not have adequate quality assurance controls in place to ensure the accuracy of Federal Employee's Compensation Act (FECA) Actuarial Liability calculated by USCP. (B4002)
- OFM was not provided property information by PAMD (Property Asset Management Division). (C3005)
- Cash differences identified by OFM are not resolved timely. (A3001 & A4006)

We recommend that the CAO implement policies and procedures covering all matters impacting USCP's financial statement and yearend closing activities and take steps to document and consistently implement new activities throughout USCP.

**Status of Recommendation: Some Progress.**

OFM has policies and procedures in place however the manpower shortage prevented effective implementation and monitoring of procedures.

**Management Response:**

USCP has taken proactive steps to ensure the compilation of financial statements and yearend processing follows a disciplined structured process. Steps taken include development of a timeline for completion of major milestones for completion of a full-set of financial statements and the utilization of contractual support services to develop a comprehensive financial statement compilation guide.

**3. USCP did not have policies and procedures to ensure coordination between the Office of General Counsel (OGC) and OFM.**

To comply with Statement of Federal Financial Accounting Standards No. 5, Accounting for Liabilities, and No. 12, Recognition of Contingent Liabilities Arising from Litigation, management is responsible for adopting policies and procedures to identify, evaluate, and account for litigation, claims and assessments as a basis for the preparation of financial statements in conformity with generally accepted accounting principles. Coordination between OGC and OFM will allow OFM to consider the need for appropriate financial statement disclosure.

We recommend that the CAO develop and implement policies and procedures to facilitate the flow of information from the General Counsel to OFM.



<p><b>Status of Recommendation: Some Progress.</b></p> <p>While OGC did provide a legal letter to the auditor in a timely manner, further improvement is required regarding communication between OGC and OFM for litigation, claims, and assessments in order to ensure timely and accurate financial reporting.</p>	<p><b>Management Response:</b></p> <p>Communication and collaboration between the Office of Financial Management (OFM) and Office of General Counsel (OGC) has improved significantly, and a standard operating procedure has been drafted to formalize the sharing of information between the Office of Financial Management and the Office of the General Counsel. This procedure clearly identifies the responsibilities of both organizations, and the type and timing of required reporting.</p>
---	---

<p><b>4. USCP was unable to reconcile property information from the accounting system with information in the new property management system. (C4005)</b></p> <p>To comply with the request to produce a balance sheet in FY 2006, OFM created a Property, Plant, and Equipment schedule used for the balance sheet line item. This schedule was created by using property data in the accounting system and confirming the data with property custodians in what OFM thought was the best data available. Substantive testing of the accounting system data revealed inconsistencies with other sources of evidence in which there should have been collaboration. Lack of coordination between Property Asset Management Division (PAMD) and OFM has created a condition in which lack of internal controls will prevent the accurate recording of information regarding asset recognition, as defined by the Statement of Federal Financial Accounting Standards (SFFAS) #6. Other weaknesses noted in Property Management include; a lack of communication procedures for when assets are transferred, removed from service, disposed of, or significant modifications are made that either change the nature of the asset or impact the life expectancy.</p> <p>We recommend that the CAO continue efforts to integrate the data between the accounting system and property management system. Additionally, policies and procedures for regular and systematic communication and coordination between PAMD and OFM must be created and implemented to facilitate asset recognition and current status of assets. Lastly, all property custodians must have real time access to the property management system to ensure that all data is accurate regarding the disposition and location of all USCP property.</p>	
<p><b>Status of Recommendation: Not Started.</b></p>	<p><b>Management Response:</b></p> <p>The implementation of a fully integrated Financial and Asset Management system has not been completed due to a shortage of funds. Until this automated integration can be accomplished, manual processes will be required. Within USCP, the Office of Logistics and Office of Financial Management have taken the following steps to facilitate asset recognition and current status of assets between the financial and asset management systems:</p> <ol style="list-style-type: none"> <li>1. Established a process to provide copies of all</li> </ol>

	<p>awards involving accountable property to Accounting and Property Management staffs to ensure timely and accurate recording.</p> <p>2. Utilized a bar-code numbering system, placed on accountable property, as the common data element of the [REDACTED] and [REDACTED] systems. Accountable property created into [REDACTED] must have an associated [REDACTED] barcode to ensure the systems remain in sync.</p> <p>3. Developed a standard operating procedure that will facilitate communication between the Property Management Division and the Office of Financial Management; ensuring that property is recorded into both systems as appropriate, and supporting ongoing reconciliations of accountable property.</p>
--	---

### Finding No. 3: Information Systems

**Summary Status:**    **Reportable Condition**  
**Prior and New Conditions**  
**Substantial Progress made on all**  
**prior conditions**

In FY 2005, seven conditions existed that cumulatively resulted in a reportable condition in the internal controls report. Based on procedures performed for FY 2006, we found that progress was made on all seven conditions and subsequently each was closed. This year eight new conditions were identified, some of which contained updates and clarification related to existing conditions. The cumulative risk associated with these eight conditions is being reported as a Reportable Condition.

#### Status of Existing Conditions from FY 2005 Internal Controls Report:

<p><b>1. USCP OIS does not have adequate separation of duties.</b></p> <p>A draft policy and matrix has been created covering segregation of duties within OIS, however it has not been implemented.</p> <p>We recommend that policies and procedures for separating incompatible duties be approved by management and implemented.</p>	
<p><b>Status of Recommendation: Closed.</b></p> <p>Management implemented the segregation of duties restrictions for IT administration functions that were in draft during the prior year review.</p>	<p><b>Management Response:</b></p> <p>USCP management concurs with this closure.</p>

**2. Environmental controls within the computer room are inadequate.**

Issues with the environmental controls over the computer room in the Headquarters building were noted. The headquarters building and the computer room are undergoing renovations. During the renovation period the environmental controls did not meet best practices, but OIS has planned upgrades that would improve controls as part of the renovation process.

We recommend that the environmental controls in the computer room are reviewed as part of a certification and accreditation process for the general support system. During that process management should assess the risk associated with the computer room's environmental controls and make improvements as appropriate.

**Status of Recommendation: Closed.**

The renovation of the computer room in the Headquarters building is nearly complete. Only minor issues were identified during this year's review and management is currently implementing plans to address these known issues. These minor issues were communicated verbally to management.

**Management Response:**

USCP management concurs with this closure.

**3. No computer security awareness training program exists.**

USCP should develop and implement security awareness training policy and procedures. All employees who have computer access should be required to attend security awareness training both initially when they are hired and annually for refresher training.

**Status of Recommendation: Closed.**

A computer security awareness training program was implemented for information system users. See current year condition #10 related to user participation in the training program.

**Management Response:**

USCP management concurs with this closure.

**4. In the prior year, it was noted that access controls and system software controls needed improvement. Specifically we noted that:**

a) Access controls are not adequate to ensure that:

- Access authorizations are:
  - Documented on standard forms and maintained on file,
  - Approved by senior managers, and
  - Securely transferred to security managers.
- Rules of behavior are signed by users before granting access to information systems.
- Generic accounts are not used for systems access.

We recommend that USCP develops policies and procedures for adding new users to the system which should include a standard user access authorization form. This form should be signed by a new user's manager and retained on file. Also new users should be required to sign a Rules of Behavior document that outlines acceptable uses of the information system before access is granted. All accounts should be assigned to an individual and not to a group of users to ensure accountability.

- b) We further noted that controls are not adequate to ensure that security is notified immediately and users are removed when they are terminated or transferred. During our review we identified many accounts that related to employees who no longer required access. The Information Security Officer performs quarterly checks for accounts and a full account review annually. The annual account review procedures appear to identify many exceptions. This indicates that the normal operating procedures for identifying accounts that are no longer required are not working effectively.

We recommend that management ensure access right for all terminated employee is removed in a timely manner, and that reviews of account listings and inactive accounts are performed timely.

- c) Finally we noted that system software controls are not adequate to ensure that information systems are configured in accordance with guidance for Federal information systems.

We recommend that management ensure that a standard security benchmark for all systems is developed and implemented. Organizations such as the National Institute for Standards and Technology (NIST) and the Center for Internet Security (CIS) provide guidance on security benchmark for Federal government systems.

**Status of Recommendation: Closed.**

Management has made substantial progress towards addressing these issues. Therefore to provide more clarity on the remaining issue, this finding was closed and section c) was re-issued in current year condition #9.

**Management Response:**

- a) USCP management concurs with this closure.  
b) USCP management concurs with this closure.  
c) See USCP response to current year condition #9.

**5. The Certifications and Accreditation (C&A) process has not been fully implemented.**

So far the [REDACTED] T&A application and the Blackberry system have undergone the agency's C&A process. Other Major Applications and the General Support System have not yet been certified or accredited. The process that was used to certify and accredit [REDACTED] requires improvement because the documentation for the process is not being updated in a timely manner. The System Security Plan for [REDACTED] describes a system that has not been fully accredited and appears to contain outdated information.

We recommend management certify and accredit all of its major applications and general support systems. We further recommend that the documentation supporting each system be maintained and updated as necessary to reflect the current environment.

**Status of Recommendation: Closed.**

**Management Response:**

Management has made significant progress in implementing a C&A process. Remaining weaknesses in the C&A process are noted in current year conditions #12, #13, #14 and #15.	USCP management concurs with this closure. See USCP management responses to current year conditions #12, #13, #14 and #15.
---	--

<b>6. Management's oversight of the outsourced Federal Financial System, was not adequate.</b>  <p>The financial system of record for FY2005 was the Federal Financial System (FFS). This system was hosted and operated by the Government Accountability Office (GAO). During the reporting period USCP did not provide oversight of controls for the system and did not have procedures in place to gain assurance over system controls. Since the system was never certified and accredited for operation for USCP the understanding and acceptance of risk associated with the system was informal.</p> <p>Since FFS is no longer used by USCP, we recommend that management perform a certification and accreditation of the new financial system, and include internal control procedures that ensure outsourced system operators provide appropriate levels of security assurance for USCP.</p>	
<b>Status of Recommendation: Closed.</b>  <p>This is no longer an issue because USCP no longer uses FFS as its financial system of record. During FY2006 the transition was made to using [REDACTED] a system hosted by GSA.</p>	<b>Management Response:</b>  <p>USCP management concurs with this closure.</p>

<b>7. USCP does not have procedures for sanitizing and disposing of media containing sensitive information.</b>  <p>USCP uses the Senate's services and procedures for disposing of the majority of their computer hardware. However, we noted that there are no procedures in place for sanitizing and disposing of media that may contain more sensitive data.</p> <p>We recommend that management develop standard procedures for sanitizing and disposing of media that may contain sensitive data.</p>	
<b>Status of Recommendation: Closed.</b>  <p>Policies and procedures have been created to address the disposition of media containing potentially sensitive data.</p>	<b>Management Response:</b>  <p>USCP management concurs with this closure.</p>

**New Conditions from FY 2006 Audit Procedures:**

<p><b>8. USCP does not have policies and procedures for identifying and protecting privacy sensitive information.</b></p> <p>A Chief Privacy Officer (CPO) has not been appointed to ensure that all personally identifiable information is identified and appropriately secured. USCP management has not conducted a privacy impact assessment or documented their procedures for protecting personally identifiable information stored in major information systems.</p> <p>We recommend that USCP officially appoint a CPO and develop policies and procedures to ensure all personally identifiable information is identified and safeguarded.</p>	
<p><b>Status of Recommendation: Not Started.</b></p> <p>Current year condition.</p>	<p><b>Management Response:</b></p> <p>USCP Agrees that this is an issue and will study the facts behind this finding and give the Chief of Police options for meeting this deficiency. Those options may include the creation of a CPO FTE, appointment of a CPO as a collateral duty, or other alternatives.</p>
<p><b>9. USCP has not implemented a comprehensive security baseline configuration for its operating systems that protects against known security weaknesses.</b></p> <p>Controls are not adequate to ensure that commonly known risks are mitigated through a secure configuration of systems. Specifically we found that the configuration checklist used by the organization contains limited specific configuration settings for the organization's environment. This checklist is not comprehensive enough to ensure that all commonly known risks are identified and addressed.</p> <p>We recommend that management ensure that a standard security benchmark for all systems is developed and implemented. Organizations such as the National Institute for Standards and Technology and the Center for Internet Security provide guidance on security benchmarks for Federal government systems.</p>	
<p><b>Status of Recommendation: Not Started.</b></p> <p>Current year condition.</p>	<p><b>Management Response:</b></p> <p>USCP Agrees that this is an issue and has purchased Security Expressions, an add-on module to existing IT management software called Altiris. This will provide the capability to scan all servers and workstations for compliance with the OIS security policy, benchmarks and accepted FISMA requirements.</p>

**10. Management has not ensured that all information system users receive security awareness training and accept the system Rules of Behavior for using the USCP Network.**

Rules of Behavior for the USCP Network are documented and made available to all users in the OIS Policy Handbook. However, users are not required to officially accept the Rules of Behavior until they participate in the online security awareness training program. Through sample testing we noted that 6 out of 45 users (13%) had not yet completed the security awareness training. Additionally, we noted that only USCP employees are required to take the security awareness training. Contractors working for USCP and using the Network are not required to take security awareness training.

We recommend that management ensure that all system users (including contractors) receive security awareness training on an annual basis, and that management develops procedures to ensure all users agree to abide by the Rules of Behavior for using USCP systems.

**Status of Recommendation: Not Started.**

Current year condition.

**Management Response:**

USCP Agrees that this is an issue, and in the future, will require that contractors take security awareness training.

The OIS policy manual included the 'Rules of Behavior' that all USCP employees agree to when taking the security awareness training.

The 'Rules of Behavior' document is currently under the standard USCP internal review and approval process.

**11. Management has not ensured that all system users for the major financial applications [REDACTED] and [REDACTED] have officially acknowledged and accepted the system specific Rules of Behavior.**

The current procedures for distributing and ensuring that major application users acknowledge system specific Rules of Behavior requires that all users review the rules individually and reply to an email stating they acknowledge the requirements. This procedure is currently in place for [REDACTED] and is soon to be implemented for [REDACTED]. However, management does not have procedures in place to ensure that all system users comply and agree to abide by the Rules of Behavior. The [REDACTED] system has been in place since October 2005 and during our sample testing, management was not able to provide evidence for 6 out of 45 selected users having acknowledged the system rules of behavior.

We recommend that management develop new procedures to ensure that all users of major financial applications review and acknowledge system specific Rules of Behavior prior to gaining system access.

**Status of Recommendation: Not Started.**

Current year condition.

**Management Response:**

USCP management has disseminated the [REDACTED] and [REDACTED] Rules of Behavior and will ensure that all system users provide written acknowledgement that they have read, understand

	and agree to the Rules of Behavior. OFM has also updated its standard operating procedures to ensure that all new system users acknowledge the rules prior to gaining access to the [REDACTED] and/or [REDACTED] systems. This operating procedure was initiated on 15 May 2007.
--	--

**12. Management has not conducted risk assessments in accordance with industry best practices that consider a holistic view of system risks for all of their major systems.**

Controls are not adequate to ensure that the USCP conducts risk assessments in accordance with industry best practices that consider a holistic view of system risks for all of their major systems.

Specifically we found that:

- The risk assessments prepared for the WAN and LAN were conducted by an independent consultant. The risk assessment identified a number of possible threat sources in three categories; human, natural, and environmental. However, the methodology used to identify specific system vulnerabilities only utilized a vulnerability scanning tool and manual configuration reviews. This approach identified logical access control and configuration vulnerabilities. It did not identify all potential vulnerabilities that could be associated with the human, natural, or environmental threats that were identified.
- Management has not conducted a risk assessment that covers the major application, [REDACTED]
- The risk assessment procedures for the new system, [REDACTED] produced a risk matrix spreadsheet that documented potential system risks associated with implementation. However the process for identifying risks did not provide documented evidence of a standardized approach to addressing risks in a manner consistent with industry best practices. There was not evidence of a holistic approach to risk management that extended past the system implementation phase.

We recommend that management conduct risk assessments in accordance with guidelines and recommendations for protecting Federal information systems. This risk assessment process and the documented results should be integrated into a comprehensive process for Certifying and Accrediting major systems.

<b>Status of Recommendation: Not Started.</b>	<b>Management Response:</b>
Current year condition.	USCP Agrees that this is an issue, and has followed the NIST guidelines, SP 800-30 Risk Assessment Guide - in the development of its risk assessments for major applications.  The general support systems' (WAN/LAN) risk assessments were completed by an independent third party (UNISYS) which also followed the NIST guidelines. The completed risk assessment is included with the C&documentation as part of



	<p>certification process for authorization to Operate (ATO).</p> <p>USCP will continue to create and update risk assessments for major systems and general support systems, including threats and vulnerabilities impacting USCP.</p> <p>The two hosted systems, [REDACTED] / [REDACTED] which are accessed via the internet browser, will have a risk assessment done on the client to complement the LAN based risk assessment covering all USCP workstations.</p>
--	--

**13. Management has not created and approved system security plans in accordance with industry best practices that fully document the controls protecting major systems.**

Controls are not adequate to ensure that a system security plan has been created in accordance with industry best practices and approved for all major systems.

Specifically we found that:

- Management has not created a system security plan that covers the major application, [REDACTED]
- The system security plans that have been created for the WAN, LAN, and ODS systems do not include descriptions of recommended controls or specific information about how those controls have been applied to the systems.
- The system security plans for the WAN, LAN, and ODS (Which includes [REDACTED] systems have not been finalized and approved by management.

We recommend that management create system security plans in accordance with guidelines and recommendations for protecting Federal information systems. System security plans should document all controls protecting the system and the final document should be approved by management before it is integrated into a comprehensive process for Certifying and Accrediting major systems.

<p><b>Status of Recommendation: Not Started.</b></p> <p>Current year condition.</p>	<p><b>Management Response:</b></p> <p>USCP Agrees that this is an issue, and System security plans will be created for [REDACTED] and ODS; in addition to the risk assessments, and security assessment report (SAR).</p>
---	---

**14. An independent security assessment has not been conducted for controls over major information systems.**

Controls are not adequate to ensure that an independent security assessment is performed for controls listed in the system security plans for major systems as part of the certification and accreditation process.

<p>Specifically we found that there is no evidence of independent security testing of all the controls identified in the systems security plans as part of the certification and accreditation process. Additionally, the certification agent for major systems is also the system's Information System Security Officer. This puts him in the position of evaluating his own performance and does not allow for a completely independent and objective assessment.</p> <p>We recommend that management ensures that there is an independent assessment of security controls conducted as part of a comprehensive Certification and Accreditation process.</p>	
<p><b>Status of Recommendation: Not Started.</b></p> <p>Current year condition.</p>	<p><b>Management Response:</b></p> <p>USCP Agrees that this is an issue, and developed the Security Assessment Report (SAR) for T&amp;A and Blackberry - major applications. We contracted with an independent contractor, Unisys, who performed the System Testing and Evaluation (ST&amp;E) to verify USCP's SAR assessment. The WAN/LAN work was done exclusively by UNISYS. All future C&amp;A assessments will be done to make the verification process independent and objective.</p>

<p><b>15. Management has not developed a policy and procedure to track and monitor corrective actions for known system security weaknesses.</b></p> <p>Controls are not adequate to ensure that management developed a policy and procedure to track and monitor corrective actions for known system deficiencies.</p> <p>Specifically we found that management has a process to document responses and corrective actions for audit recommendations. However, this process only addresses audit issues and does not provide a mechanism for tracking and addressing all known system weaknesses such as those identified through the certification and accreditation process.</p> <p>We recommend that management develops a process to track and manage all known system weaknesses. This process should include a centralized method of documenting and managing known issues, their associated corrective action plans, and the status of change implementations.</p>	
<p><b>Status of Recommendation: Not Started.</b></p> <p>Current year condition.</p>	<p><b>Management Response:</b></p> <p>USCP Agrees that this is an issue, and Policy and procedures will be created to track and monitor the 'Plan of Actions and Milestones' (POAM) to complete corrective actions and implementations.</p>



Cotton & Company LLP  
635 Slaters Lane  
4<sup>th</sup> Floor  
Alexandria, VA 22314

P: 703.836.6701  
F: 703.836.0941  
www.cottoncpa.com

United States Capitol Police Board

### INDEPENDENT AUDITORS' REPORT ON COMPLIANCE WITH LAWS AND REGULATIONS

We were engaged to audit, in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, the statement of financial position as of September 30, 2006, and the related statement of budgetary resources of the United States Capitol Police (USCP) for the fiscal year ended September 30, 2006. In a report dated April 12, 2007 we disclaimed an opinion on those financial statements for the scope limitation described in the third paragraph therein.

USCP management is responsible for complying with laws and regulations applicable to the agency. An audit performed in accordance with *Government Auditing Standards* includes obtaining reasonable assurance that the financial statements are free of material misstatement, based upon performing tests of USCP's compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. Had we been able to perform all of the procedures necessary to express an opinion on the financial statements, other matters involving compliance with laws and regulations may have been identified and reported.

However, we are not aware of any instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

~~This report is intended solely for the information and use of the United States Capitol Police Board, USCP management, Members of the United States Congress, and the Comptroller General of the United States and is not intended to be, and should not be, used by anyone other than these specified parties.~~

COTTON & COMPANY LLP

Alan Rosenthal, CPA  
Partner

April 12, 2007  
Alexandria, Virginia