α1

Independent Auditor's Report on Internal Control

To the Inspector General of the
Corporation for National and Community Service

We have audited the financial statements of the Corporation for National and Community Service (Corporation) as of and for the year ended September 30, 2008, and have issued our report thereon dated November 14, 2008. We conducted our audit in accordance with the auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States; and, Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended.

In planning and performing our audit, we considered the Corporation's internal control over financial reporting by obtaining an understanding of relevant internal controls, determined whether these internal controls had been placed in operation, assessed control risk, and performed tests of controls in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and to comply with OMB Bulletin No. 07-04, as amended, but not for the purpose of expressing an opinion on the effectiveness of internal control over financial reporting. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act* (FMFIA) (31 U.S.C. 3512), such as those controls relevant to ensuring efficient operations. The objective of our audit was not to provide assurance on internal control. Accordingly, we do not express an opinion on the effectiveness of the Corporation's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider collectively to be a significant deficiency.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or reliably report financial data in accordance with generally accepted accounting principles such that, there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control. We consider the deficiency described below to be a significant deficiency in internal control over financial reporting.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in a more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

11710 Beltsville Drive
Suite 300
Calverton, Maryland 20705
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

Our consideration of internal control over financial reporting was for the limited purpose described in the second paragraph and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. However, we do not believe that the significant deficiency described below is a material weakness.

Significant Deficiency

CONTINUITY OF OPERATIONS

Losing the capability to process and retrieve information maintained on CNCS's computer systems can significantly impact CNCS's ability to initiate, authorize, record, process, or report reliable financial data. The purpose of service continuity controls is to ensure that, when unexpected events occur, critical operations continue without interruption or are promptly resumed. To achieve this objective CNCS should have (1) procedures in place to minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider activities performed at CNCS's general support facilities, as well as the activities performed by users of specific applications. To determine whether the disaster recovery plans will work as intended, CNCS should establish and periodically test the capability to perform its functions in disaster simulation exercises. The following weaknesses noted below describe deficiencies in business continuity controls at CNCS.

1. Application Development and Change Control:

Significant interface interoperability and unavailability issues in FY 2008 impacted the Corporation's ability to operate. Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, states that a loss of *availability* is the disruption of access to or use of information or an information system and defines security categories for information systems based on potential impact on organizations or individuals should there be a breach of security – that is, a loss of confidentiality, integrity (including authenticity and non-repudiation), or availability. By authorizing an information system for operation, an organizational official accepts *responsibility* for the security of the system and is *accountable* for any adverse impacts that may occur if the system is breached thereby compromising the confidentiality, integrity, or availability of the information being processed, stored, or transmitted. The events, noted below, led to the system outages, disrupted system availability and created an unstable computer operating environment. In order to stabilize the computer environment, management limited system availability to its customers and employees with prescheduled blackouts to its mission critical applications. These issues resulted in major system outages totaling over 20 days, within a six-month time-span beginning February 2, 2008. The financially significant systems impacted included the general ledger system, the central database for National Service Trust and participants, and the grants management system.

In January 2008, there were two major contracted system projects implemented within days of each other. Both projects were being managed by separate areas within the Corporation; the Project Management Office (PMO) managed one project and the Office of the Chief Financial Officer (CFO) managed the other. The PMO managed the implementation of the AmeriCorps Portal (a self-service, on-line AmeriCorps program support system) and the CFO managed the implementation of the general ledger system upgrade. These projects relied heavily on the functions, support and testing of Information Technology (IT) systems and components. Concurrent migration of both projects did not allow adequate time to

perform testing to identify potential load and interface issues. There was also insufficient communication among key stakeholders (PMO, Office of Information Technology (OIT), and the CFO) during the phases of implementation for the AmeriCorps Portal.

During this same period, OIT was heavily involved in addressing infrastructure support shortfalls resulting from the failed contract due to the bankruptcy of its infrastructure support contractor. There were two-thirds fewer resources available in OIT to support day-to-day operations and functions. This left very limited resources available to focus coordination and testing efforts for the system projects to ensure they did not result in any system degradation and unavailability issues. Lack of resources, communication, and the timing of the migration to the upgraded general ledger system and Portal implementation resulted in significant problems including lack of interface interoperability, unavailability and delays in processing.

CNCS had a SWAT team monitoring the system and is now in the process of developing and implementing remediation controls. CNCS upgraded the database to be compatible with the version used by the third party processor and ensure a more stable operating environment. CNCS also had an independent consultant review their controls and make recommendations to correct the weaknesses noted.

Recommendations: We recommend that the Corporation do the following:

1. Management should establish a central mechanism for coordinating and managing resources required for projects that rely on IT resources.
2. Management should consider the financial and operational impact when planning multiple system projects occurring concurrently (i.e. staffing, system load, system testing and system availability).
3. Management should effectively communicate with key stakeholders who are responsible for supporting systems to be sure that there is adequate time and resources to test.
4. For all system projects, Management should follow the documented Corporation System Development Life Cycle process.

2. Continuity of Operations Plan and Testing:

Losing the capability to process and retrieve information maintained electronically can significantly affect CNCS's ability to accomplish its mission. OMB Circular A-130 Appendix III, *Security of Federal Automated Information Resources,* states that: "Experience has shown that recovery plans that are periodically tested are substantially more viable than those that are not. Moreover, untested plans may actually create a false sense of security." CNCS participated in the Federal Emergency Management Agency (FEMA)'s exercise to test the continuity of the executive branch through testing the continuation of National Essential Functions (NEFs). However, the test was not designed to test the preparedness of CNCS to operate in the case of a CNCS specific disruption. CNCS' COOP also requires an annual COOP exercise to train and test personnel, plans and capabilities. For this reason, CNCS should follow best Federal business practices and its own procedures to minimize the risk of unplanned interruptions. CNCS should also schedule the annual testing of its plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific

applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises. The following matters were noted during our audit:

- The Corporation's Continuity of Operation Plan (COOP), was not maintained in accordance with the Corporation's policies and procedures (ISP-P-11-0705). Below are issues we noted:

  - The COOP is not updated annually in accordance with the Corporation policy. The last COOP update was in July 2006.

  - The COOP is not updated with test results or lessons learned from test exercises.

- The Corporation has documented its Continuity of Operations Plan (COOP). However, the plan has not been tested to execute the scripted responses to emergencies (Levels 1 through 4) to validate the effectiveness of the COOP and the preparedness of the Corporation to carry out its mission in the case of an emergency.

- In place of testing the COOP, the Corporation placed reliance on the evaluation of its COOP as part of the Federal Emergency Management Agency (FEMA) initiated Eagle Horizon exercise, dated May 8, 2008. However, the evaluation conducted by a third party Federal agency, did not include tests of Levels of Emergency (1 through 4) identified in the COOP. The result of the Eagle Horizon exercise was not used to update the COOP.

- The Corporation determined that the most critical function to be tested was the Corporation's ability to communicate through Blackberry devices in the event of a disaster. However, no business impact analysis was performed in support of this decision, and the COOP was not updated to include this level of testing.

- In lieu of testing the documented COOP, the Corporation performed two exercises that were specific to the BlackBerry devices. The two exercises tested the Corporation's ability to communicate with employees using this device during a disaster. The Corporation did not document test results or lessons learned from the tests performed. Neither of the BlackBerry exercise responses were scripted within the current COOP. In addition, these exercises are not consistent with the Levels of Emergency (1 through 4).

Recommendations:

1. Management should maintain the COOP and ensure that it is updated at least annually, or if major changes occur.
2. Management should perform testing in accordance with the documented Corporation COOP and Federal standards.
3. Management should document test results or lessons learned from the tests performed in order to identify gaps to be used for future updates to the plan.
4. Management should update its business impact analysis to include the communications through BlackBerry devices.
5. Management should add the results of the BlackBerry exercise to the COOP.

****

In addition, we noted other matters involving internal control and its operation that we will report to the Corporation management in a separate management letter.

Agency Comments and Our Evaluation

In commenting on the draft of this report (attached exhibit), Corporation management did not concur with the facts and conclusions in our report, but stated that our recommendations "are either in line with what we already have in place or can be readily adopted through improved documentation". We did not perform audit procedures on the Corporation's written response to the significant deficiencies and, accordingly, we express no opinion on it.

This report is intended solely for the information and use of the management of the Corporation, the Office of Inspector General, OMB, the Government Accountability Office and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Clifton Gunderson LLP

Calverton, Maryland
November 14, 2008