GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL

DISTRICT OF COLUMBIA
UNEMPLOYMENT COMPENSATION FUND

Management Letter Report
Years Ended September 30, 2012, and 2011

CHARLES J. WILLOUGHBY
INSPECTOR GENERAL

OIG No. 13-1-10BH(a) **May 3, 2013**

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

May 3, 2013

The Honorable Vincent C. Gray
Mayor
District of Columbia
Mayor's Correspondence Unit, Suite 316
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

The Honorable Phil Mendelson
Chairman
Council of the District of Columbia
John A. Wilson Building, Suite 504
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Dear Mayor Gray and Chairman Mendelson:

As part of our contract for the audit of the District of Columbia's general purpose financial statements for fiscal year (FY) 2012, KPMG LLP (KPMG) submitted the enclosed final management letter report on the District of Columbia Unemployment Compensation Fund (Fund) for years ended September 30, 2012, and 2011 (OIG No. 13-1-10BH(a)). This report sets forth KPMG's comments and recommendations to improve internal control or result in other operating efficiencies, which are summarized in Attachment A of the enclosed report.

KPMG identified significant deficiencies in general information technology controls and various information technology systems. Management concurs with the facts of all the findings.

If you have questions or need additional information, please contact Ronald W. King, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,

Charles J. Willoughby
Inspector General

CJW/ws

Enclosure

cc: See Distribution List

DISTRIBUTION:

Mr. Allen Y. Lew, City Administrator, District of Columbia (via email)
Mr. Victor L. Hoskins, Deputy Mayor for Planning and Economic Development, District of Columbia (via email)
The Honorable Kenyan McDuffie, Chairperson, Committee on Government Operations, Council of the District of Columbia (via email)
Mr. Brian Flowers, General Counsel to the Mayor (via email)
Mr. Christopher Murphy, Chief of Staff, Office of the Mayor (via email)
Ms. Janene Jackson, Director, Office of Policy and Legislative Affairs (via email)
Mr. Pedro Ribeiro, Director, Office of Communications, (via email)
Mr. Eric Goulet, Budget Director, Mayor's Office of Budget and Finance
Ms. Nyasha Smith, Secretary to the Council (1 copy and via email)
Mr. Irvin B. Nathan, Attorney General for the District of Columbia (via email)
Dr. Natwar M. Gandhi, Chief Financial Officer (1 copy and via email)
Mr. Mohamad Yusuff, Interim Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
Ms. Yolanda Branche, D.C. Auditor
Mr. Phillip Lattimore, Director and Chief Risk Officer, Office of Risk Management (via email)
Mr. Steve Sebastian, Managing Director, FMA, GAO, (via email)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives, Attention: Bradley Truding (via email)
The Honorable Darrell Issa, Chairman, House Committee on Oversight and Government Reform, Attention: Howie Denis (via email)
The Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and Government Reform, Attention: Yvette Cravins (via email)
The Honorable Thomas Carper, Chairman, Senate Committee on Homeland Security and Governmental Affairs, Attention: Holly Idelson (via email)
The Honorable Tom Coburn, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs, Attention: Katie Bailey (via email)
The Honorable Mark Begich, Chairman, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia, Attention: Cory Turner (via email)
The Honorable Rand Paul, Ranking Member, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia
The Honorable Harold Rogers, Chairman, House Committee on Appropriations, Attention: Amy Cushing (via email)
The Honorable Nita Lowey, Ranking Member, House Committee on Appropriations, Attention: Laura Hogshead (via email)
The Honorable Ander Crenshaw, Chairman, House Subcommittee on Financial Services and General Government, Attention: Amy Cushing (via email)
The Honorable José E. Serrano, Ranking Member, House Subcommittee on Financial Services and General Government, Attention: Laura Hogshead (via email)

The Honorable Barbara Mikulski, Chairwoman, Senate Committee on Appropriations, Attention: Ericka Rojas (via email)
The Honorable Richard Shelby, Ranking Member, Senate Committee on Appropriations, Attention: Dana Wade (via email)
The Honorable Frank Lautenberg, Chairman, Senate Subcommittee on Financial Services and General Government, Attention: Marianne Upton (via email)
The Honorable Mike Johanns, Ranking Member, Senate Subcommittee on Financial Services and General Government, Attention: Dale Cabaniss (via email)
Mr. Paul Geraty, CPA, Public Sector Audit Division KPMG LLP (1 copy)

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

January 25, 2013

Inspector General of the Government of the District of Columbia
Director of the Office of Unemployment Compensation in the Government of the District of Columbia
The Government of the District of Columbia

We have audited the financial statements of the Government of the District of Columbia's Unemployment Compensation Fund (the Fund), as of September 30, 2012 and 2011, and the related statements of revenues, expenses and changes in net assets and statements of cash flows for the years then ended (here in after referred to as the basic financial statements) and have issued thereon dated January 25, 2013. In planning and performing our audit of the basic financial statements of the Fund, in accordance with auditing standards generally accepted in the United States of America, we considered the Fund's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the basic financial statements but not for the purpose of expressing an opinion on the effectiveness of the Fund's internal control. Accordingly, we do not express an opinion on the effectiveness of the Fund's internal control.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and suggested recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in Attachment A.

In addition, we identified certain deficiencies in internal control that we consider to be a significant deficiency and communicated to the Mayor, the Council of the Government of the District of Columbia, and the Inspector General of the Government of the District of Columbia in writing as of January 25, 2013.

We would be pleased to discuss the attached comments and recommendations with you at any time.

This communication is intended solely for the information and use of the Fund's management, and the Inspector General of the Government of the District of Columbia, and others within the organization, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Attachment A

Comment 1: Weaknesses in the Fund's General Information Technology Controls

Background:

General Information Technology Controls (GITCs) provide the foundation for a well-controlled technology environment that supports the consistent processing and reporting of operational and financial data in accordance with management's directives. Our audit included an assessment of selected GITCs in four (4) key control areas: (1) Access to Programs and Data, (2) Program Changes, (3) Program Development, and (4) Computer Operations. During our fiscal year (FY) 2012 audit, the following findings were identified:

General Information Technology Controls:

1. Access to Programs and Data – Inconsistent Password Configuration Settings

Conditions:

During our testwork, we determined that the Office of the Chief Technology Officer (OCTO) management had not updated its policy that defines the minimum password configuration requirements for District of Columbia (DC) IT systems since 2004. Additionally, further inquiry and inspection procedures performed by the audit team indicate that the policy was not effectively communicated to responsible personnel. Specifically, we noted the following:

a. OCTO's Password Management Policy, last revised in November 2004, does not require that systems be configured to automatically lock out user accounts after a predefined number of invalid log-on attempts.

b. There were various inconsistencies between the requirements outlined in the OCTO Password Management policy and configurations set within the in-scope applications and their supporting databases and operating systems.

c. There is potentially confusing language around the scope of the policy, which indicates it is to include "all District Government agencies and all users of the DC Government computing equipment" when in fact the non-mayoral entities such as the Office of the Chief Financial Officer (OCFO), which are user organizations of computing equipment and services provided by OCTO, are not under the discretion of this policy.

As this was a finding in both FY 2010 and FY 2011, OCTO management implemented a revised Password Management Policy, effective on August 31, 2012, which included a requirement for account lockout settings as well as defines clearly the scope of the policy in remediation of the issues noted above. However, a deficiency in the control environment existed for the period during the year under audit of October 1, 2011 through August 31, 2012.

Criteria:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, section Identification and Authentication (IA-5) states:

"The information system, for password-based authentication:

(a) Enforces minimum password complexity of […organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

(b) Enforces at least a […organization-defined number of changed characters] when new passwords are created;

(c) Encrypts passwords in storage and in transmission;

(d) Enforces passwords minimum and maximum lifetime restrictions of […organization defined numbers for lifetime minimum, lifetime maximum]; and

(e) Prohibits password reuse for [[an] organization-defined number [of]] generations."

Further, section Access Control (AC-7) states:

"The information system enforces a limit of [[an] organization-defined number [of]] consecutive invalid access attempts by a user during … [[an] organization-defined time period]…The information system automatically […locks the account/node for an […organization-defined time period] [or] delays [the] next login prompt according to [[an] organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded."

Cause/Effect:

Prior to the implementation of its revised password policy noted in the condition above, Fund management had not established a formalized process for periodically reviewing, updating, and communicating requirements posed by the OCTO Password Management Policy. Additionally, management has not taken steps to ensure that policies and their supporting procedures align in scope and content with other policies enacted across the District.

As a result, there was an increased risk that password configuration settings would be implemented inconsistently, if at all. Weakly configured password settings increase the risk that unauthorized users can access sensitive system functions, which can negatively impact the confidentiality, integrity and availability of application data.

Recommendations:

We recommend that Fund management:

- Continue to reassess and revise, as necessary, the password policy put in place in remediation of the deficiency noted above, and
- Should ensure that this policy is adhered to by IT systems and infrastructure within the scope of the policy.

Management's Response:

Management concurred with the above finding. As noted above, OCTO management implemented a revised Password Management Policy, effective on August 31, 2012, which remediated the deficiencies noted in the NFR by including a requirement for account lockout settings and defining clearly the scope of the policy in remediation of the issues noted above. The revised policy governs password management going forward. OCTO concurs with the finding because the revised policy was not in effect during the year under audit of October 1, 2011 through August 31, 2012.

Various IT Systems

1. <u>Access to Programs and Data for the Budget and Reporting Tracking System (BARTS) and District Unemployment Tax Administration System (DUTAS) – Terminated Employees in BARTS and DUTAS</u>

Condition:

We tested management's process for removing access to the District of Columbia Government's computer systems after employee separation by comparing the active user listings from BARTS and DUTAS to the population of 92 Department of Employment Services (DOES) separated employees from FY 2012, and noted two instances were separate employee's access was not removed after their date of termination. In performing additional evaluation procedures, we noted that these employees did not log into the BARTS and DUTAS application after their termination dates. Further, in October 2012 we observed the BARTS and DUTAS accounts of the terminated users and noted that the two accounts were deactivated. While the evaluation procedures suggest that these accounts were not used in an unauthorized manner, management's failure to remove or disable them upon termination represents a control deficiency that continued to exist until the accounts were deactivated.

Criteria:

NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995, states:

"Effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations. This is augmented by the process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations. Finally, there are considerations involved in the timely modification or removal of access and associate issues for employees who are reassigned, promoted, or terminated, or who retire."

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, section Physical and Environmental Protection (PE-2) states:

"The organization manages information system accounts, including…establishing, activating, modifying, disabling, and removing accounts…notifying account managers when…information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;…and deactivating…accounts of terminated or transferred users."

Cause/Effect:

The process for removing terminated employees' user access from the BARTS and DUTAS application as defined within the Office of the Chief Financial Officer (OCFO) Financial Policies and Procedures was not followed for the two individuals noted within the condition above. Specifically, the Security Administrators for BARTS and DUTAS did not receive timely notification from management regarding the separation of the two employees and therefore were not aware of the need to remove access.

Without consistently following the process for timely communication of and removal of system access for separated employees, the risk exists that a separated person with malicious intent, or another person with knowledge of the separated person's logon credentials, may be able to use the account to alter the integrity of application data contained within applications such as BARTS and DUTAS.

Recommendations:

We recommend that Fund management:

- Re-emphasize the established process for communicating separations and removing separated employees' user access to the BARTS and DUTAS application with all parties responsible for control performance to increase the consistency with which the process is followed.

- Consider implementing a monitoring process by which weekly reports of terminated employees are received from human resources and compared to active users within in-scope applications so that any matches can be further researched and have access removed as necessary.

- Periodically monitor control performer adherence to these control activities.

Management's Response:

Management concurs with the facts of the finding. The two users in question were not removed from the system in a timely manner due to an unusual miscommunication between Human Resources and the OIT department. It should however be noted that this issue would not have gone undiscovered, due to DOES's existing semiannual system access review process.

2. Access to Programs and Data for the District Online Compensation System (DOCS) and the District Unemployment Tax Administration System (DUTAS) – DOCS and DUTAS Application Administrator Access

Condition:

We observed the entire population of Security Administrators for the DOCS and the DUTAS applications and noted two of the DUTAS and one of the DOCS users with access to administer security possessed conflicting responsibilities as either developers or business end users who had access to administer security for the applications. Specifically, we noted that two developers had access to administer security for the DUTAS application and one business user had the ability to administer security for the DOCS application. Fund management has deemed the access of these individuals appropriate to perform this function and has indicated the individuals only possess this level of access in a backup capacity rather than as the primary security administrators for the applications. However, lack of segregation of duties between these functions represents a weakness in the internal control environment for these two applications.

Criteria:

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, section Access Control (AC-5) states:

"The organization:

(a) Separates duties of individuals as necessary, to prevent malevolent activity without collusion;

(b) Documents separation of duties; and

(c) Implements separation of duties through assigned information system access authorizations.

Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided amount different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions…"

Cause/Effect:

Based on a consideration of priorities and limited resources, management has not yet allocated the resources required to develop and implement segregation of duties controls that mitigate the risks associated with the condition. This includes, but is not limited to, the segregation of program development and business end user roles from production application administration roles among different individuals,

and/or other mitigating controls such as monitoring the activities of the individuals with administrative level access.

Specifically, the two developers noted with access to administer security to DUTAS are the only two OIT personnel currently aligned to support DUTAS. Additionally, the business end user with access to administer security for DOCS was placed into this role as a backup administrator in the past when this function was entirely the responsibility by Unemployment Insurance (UI) personnel. Prior to FY 2012, Fund management moved the primary security administer role for DOCS out of UI into the Office of Information Technology (OIT) and will continue to work to move the backup security administrator role into this department as well in remediation of the condition noted above.

As a result, the lack of segregation of duties between those with business responsibilities and those with administrator levels of access may provide the business user with access to more functional transactions than are required to perform their job based on their job responsibility. The individual may have access to bypass certain system or process-based controls within the applicable business processes.

Furthermore, the lack of segregation of program development roles from production system administration roles increases the risk that certain data or configuration changes could be made directly within the applications, by passing established change control procedures. Such changes, if not authorized, tested, and properly implemented, could have adverse effects on the availability or processing/data integrity of the application.

Additionally, there is a risk that the established process for user access management could be circumvented by individuals with inappropriate security administrator access, which could result in users gaining access to privileges in DOCS and DUTAS that may not be authorized or even required.

However, Fund management has indicated that there were no noted cases in which the access rights held by the individuals noted in the condition were utilized to make unauthorized changes in access within the applications.

Recommendations:

We recommend that Fund management develop and implement controls that establish one or more of the following:

- Document and periodically review policies and procedures that define the job functions authorized by management to have access to the DOCS and DUTAS administrator roles;
- Define organizational and logical segregation of duties related to production system support user security administration, and general business user roles among different individuals;

  and/or

- Implement one or more independently operated monitoring controls over the activities of individuals with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.

Additionally, Fund management should periodically monitor control performer adherence to these control activities.

Management's Response:

Management concurs with the facts of this finding. Access to DUTAS Security administration (ability to assign transaction windows to users) should be viewed within DOES's context. Two of the individuals

mentioned are the only OIT DUTAS system support personnel. The third user has a compliance role. Segregation of duties is already implemented based on the fact that there are other administrators assigned to other systems who do not have jurisdiction in DUTAS.

3. Program Changes and Access to Administer the Database for the DOCS – DOCS Access to Migrate Changes and Database Administration Segregation of Duties

Condition:

We reviewed the entire population of individuals with access to modify data and make application program changes to the DOCS application and determined:

1) One individual with development responsibilities has access to migrate changes to production for DOCS through access to the load library using the employee's own login ID to the system. This user also has access to modify the backend data for the DOCS application.

2) A series of users were determined to no longer require access to DOCS production datasets, which provides users the ability to modify production data and programs. Those with access include three DOES personnel and eleven OCTO personnel for the DOCS application.

Criteria:

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009, section Access Control (AC-5) states:

"The organization:

(a) Separates duties of individuals as necessary, to prevent malevolent activity without collusion;

(b) Documents separation of duties; and

(c) Implements separation of duties through assigned information system access authorizations.

Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions…"

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009, section Access Control (AC-6) states:

"The organization employs the concept of last privilege, allowing only authorized accesses for users (and processes on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

Recommended control enhancements within this section include:

"The organization requires that users of information system accounts, or roles, with access to [for security functions defined as appropriate by the organization], use of non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions."

Cause/Effect:

The individuals noted above all required this level of access at some point in the past. However, the current DOES application periodic review of access focus entirely on application-level access rights and does not consider access to the mainframe datasets that underlie the application. As a result, there has been no formal process to review and ensure appropriateness of these access rights in the past.

Furthermore, the lack of segregation of duties controls increases the risk that developers can create and apply changes to application programs, data, and/or the configurations of the underlying database schema to the production environment that have adverse effects on the availability or processing/data integrity of the application without the Fund management's awareness or approval.

The inappropriate access of individual users, whose access is not commensurate with their responsibilities, increases the risk that unauthorized or inappropriate modifications could be applied to the programs, data, and configurations that have adverse effects on the availability or processing data integrity of the application without management's awareness or approval.

Recommendations:

We recommend that Fund management enhance the current DOES application periodic access review process to review those individuals and accounts with access to make changes to production mainframe supporting DOCS. This review should be consistently performed and documented by data owners with knowledge of the appropriateness of the access rights held to these mainframe datasets and without access to administer security at the Resource Access Control Facility (RACF) mainframe level.

Management's Response:

Management concurs with the facts of this finding. Users who had access to datasets in question had their roles transitioned to a different group and hence, no longer needed such access. Others served as back administrators. Affected users' accesses were removed as part of [DOES's] October system access review exercise.

4. Access to Programs and Data for PeopleSoft, the Procurement Automated Support System (PASS), and the Benefit Audit, Reporting, and Tracking System (BARTS) – OCTO Data Center 1 Physical Access

Condition:

In our testwork over the physical access controls for the OCTO Data Center 1 (ODC1), we noted that at least 133 individuals held badge access to the server room for a portion of FY 2012 when it was not required in accordance with their job responsibilities. Of these 133 individuals:

- Four were members of the Department of Human Services (DHS) and nine were members of OCTO that required access to the data center previously; however, at the time of review, no longer required this level of access.
- 120 individuals were members of other agencies that were granted access to the data center without the consultation of the OCTO management.

Criteria:

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009, section Physical and Environmental Protection (PE-2) states:

"The organization:

a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

b. Issues authorization credentials;

c. Reviews and approves the access list and authorization credentials [at a frequency defined as appropriate by the organization], removing from the access list personnel no longer requiring access."

Cause/Effect:

The administration of physical access to the ODC1 server room is managed by agencies outside of OCTO's purview, and as such, OCTO has been unable to enact governance protocols and controls efficiently to ensure that only those individuals necessitating access to the server room in accordance with their job responsibilities are granted and retain such access.

As a result, if individuals obtain/retain inappropriate physical access to networking devices, operating consoles, host computers and peripherals located in the data center, which is not required in accordance with their job responsibilities, there is an increased risk that this equipment could be damaged and/or removed, impacting hosted applications' availability and/or operational integrity.

Additionally, there is the potential for an individual's logical access granted within environments hosted at the data center will be greater than is required per their job responsibilities, especially in cases where console machines with administrative privileges can be accessed inappropriately.

Recommendations:

We recommend that Fund management move forward with current plans to take ownership of the physical access administration processes for ODC1 to allow for more efficient and effective completion of control processes in the areas of new badge access provisioning, badge access termination, and badge access periodic review. This will assist in ensuring that this access is granted to and retained by only those individuals requiring this level of access in accordance with their job responsibilities.

Specifically, Fund management should ensure that the following control activities are implemented as well as consistently performed and documented:

- Formal approval of new and temporary badge access requests to ODC1 by management personnel with appropriate knowledge of those who require this level of access;
- Timely removal of new and temporary badge access for those individuals who have separated from the District or transferred job responsibilities to a role no longer requiring such access; and,
- Periodic review (at least semi-annually) of those individuals with badge access to the ODC1 by management personnel with appropriate knowledge of those who require this level of access.

Management's Response:

Management concurs with the facts of this finding. Management has initiated development and implementation of new policies and procedures designed to ensure that access to the ODC1 data center is

granted to and retained by only those individuals requiring this level of access in accordance with their job responsibilities. The new policies and procedures will require consistent execution and documentation of the following control activities:

- Formal approval of new and temporary badge access requests to ODC1 by management personnel with appropriate knowledge of those who require this level of access;
- Timely removal of new and temporary badge access for those individuals who have separated from the District or transferred job responsibilities to a role no longer requiring such access; and,
- Periodic review (at least semi-annually) of those individuals with badge access to the ODC1 by management personnel with appropriate knowledge of those who require this level of access.

Activities now underway to support implementation of the new policies and procedures include removing agencies and service groups not needing access from the access list; periodically reviewing the access list to ensure only personnel whose job functions require access are on the list; and installing video-surveillance monitoring and a separate key-card access system for all doors at the ODC1 datacenter.

Control performers will be training on the new policies and procedures, and management will monitor adherence to the control activities. This remediation is expected to be complete by the end of the second quarter of FY 2013.

5. Access to Programs and Data for the DUTAS application – New User Access Authorization Forms

Condition:

For one of three new users granted access to the DUTAS application during FY 2012 and selected for testing, there was no notation on the access request form submitted for this user and was granted access greater than read-only into the application. While we determined the access rights assigned to be appropriate for the user identified above, this lack of documentation represents a weakness in the new user provisioning process.

Criteria:

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995, states:

"Effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations. This is augmented by the process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations. Finally, there are considerations involved in the timely modification or removal of access and associated issues for employees who are reassigned, promoted, or terminated, or who retire."

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009, section Physical and Environmental Protection (PE-2) states:

"The organization manages information system accounts, including…establishing, activating, modifying, disabling, and removing accounts…notifying account managers when…information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;…and deactivating…accounts of terminated or transferred users.

Systems operations staff will normally then use the account request to create an account for the new user. The access levels of the account will be consistent with those requested by the supervisor. This account will normally be assigned selected access authorizations. These are sometimes built directly into

applications, and other times rely upon the operating system. "Add on" access applications are also used. These access levels and authorizations are often tied to specific access levels within an application."

Cause/Effect:

The process for granting access to the DUTAS application dictates that an access request form indicating the specific DUTAS privileges should be completed prior to assignment of access. However, in cases in which specific access rights requested are not included in the access request form submitted, less formal methods of determining the access to be provisioned, such as verbal conversations with appropriate approvers, are utilized by the security administrator to ensure that access provisioned is appropriate. These undocumented mechanisms were used to determine the specific access rights to be provisioned in the case of the user noted in the condition above.

While the access rights assigned to the user identified in the condition above were determined to be appropriate mitigating the risk in this particular case, if specific and approved privileges required for new users are not clearly documented and communicated during the new user access management process, there is a risk that individuals will be assigned access to the system that is not appropriate or is excessive based on job responsibility. As a result, users may obtain and retain inappropriate access to information system resources and advertently or inadvertently use various functions to process transactions or change data within the system that is not authorized or compromises the integrity of the application and its data.

Recommendations:

We recommend that Fund management:

- Re-emphasize the established process for granting new user access to the DUTAS application and formally indicate and approve the specific access that should be granted to new DUTAS users with all parties responsible for control performance to increase the consistency with which the process is followed.
- Should periodically monitor control performer adherence to these control activities.

Management's Response:

Management concurs with the facts of this finding. The particular access requests in question did not indicate specifically which transaction windows were being requested. It should however be noted, that the request did indicate the users' job roles. The job role, common to both users, is known, as a matter of default, to require read only access to screens required for such a role to perform associated duties. This finding has however been noted and future requests will be required to check off all appropriate options checkboxes in the quickbase application before implementation. No inappropriate access was granted.

6. Access to Programs and Data for BARTS – BARTS Operating System and Database Administrative Access

Condition:

We reviewed the entire population of accounts with operating system and database administrative privileges supporting the BARTS application and noted the following conditions:

1. Eight system and generic accounts with active access to administer the operating system no longer required these administrative privileges. Per inquiry of Fund management, these accounts have not been procedurally utilized during FY 2012 and knowledge of the passwords has been restricted to appropriate individuals. However, the active access for these accounts, which is no longer necessary, represents a weakness in the control environment.

2. Due to the configuration of the Windows SQL Server 2000 environment supporting the BARTS database, access to the "SA" generic account is shared by three individuals in addition to their unique accounts. Additionally, eight individuals with Domain Administrator privileges have access to administer the database supporting the BARTS application through the BUILTIN\Administrators conduit. Per inquiry of management, the individuals with Domain Administrator privileges have not procedurally used their access to administer the database; however, their access to administer the database, which does not commensurate with their job responsibilities, represents a weakness in the control environment.

Criteria:

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995, states:

"Effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations. This is augmented by the process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations."

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009, section Access Control (AC-6) states:

"The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

Recommended control enhancements within this section include:

"The organization requires that users of information system accounts, or roles, with access to [for security functions defined as appropriate by the organization], use of non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any us of privileged accounts, or roles, for such functions."

Cause/Effect:

Fund management has not implemented formal policies and procedures to monitor accounts with privileged access and ensure that system and generic accounts that no longer require privileged access have been disable or deleted timely. Additionally, due to system limitation, management cannot disable or remove some default privileged accounts, for which monitoring policies and procedures were not implemented.

The use of a generic account to perform server administration could result in a lack of accountability for use of the account and difficulty in ensuring control over the access.

In addition, the existence of dormant accounts that no longer require access could result in using accounts which are not monitored or reviewed, and account login information could be obtained and used in an unauthorized manner.

Furthermore, access to administer the database by the domain administrators could inadvertently cause harm or negatively impact the database when performing administrator level functions on the network or Windows Server. In addition, inappropriate users with access to administer the database could apply back-end changes and, as a result, negatively impact the confidentiality, integrity, and availability of the system and data.

Recommendations:

We recommend that Fund management establish and implement formalized operating system and database security policies that, at a minimum, include consideration for following:

- A process to log a ticket each time the "SA" account or other privileged system account is used and monitor the "SA" or other account activity against a change control log. Also ensure that passwords to "SA" or other privileged accounts are periodically changed and immediately changed upon the separation of an individual with knowledge of the password.
- A periodic review of all accounts with access to administer the operating system and database, which verifies the appropriateness of both generic accounts and individuals, including individuals who have privileged access assigned through conduit accounts (e.g., BUILTIN\Administrators).

Management's Response:

Management concurs with the facts of this finding. The BARTS system/Database administrator would be required to extract privilege access logs, on an at least semiannual basis, and submit to IT Security for review.

7. Access to Programs and Data for BARTS – BARTS Periodic Access Review Segregation of Duties

Condition:

KPMG inspected the User Access Review that was performed for the BARTS application on 6/6/2012 and noted that the review was performed by a user who has the logical access rights required to administer security for the BARTS application. This combination of responsibilities within the access review process represents a segregation of duties conflict.

Criteria:

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, section Account Management (AC-2) states:

"The organization manages information system accounts including:

a. Identifying accounts types (i.e., individual, group, system, application, guest/anonymous, and temporary);

b. Establishing conditions for group membership;

c. Identifying authorized users of the information system and specifying access privileges;

d. Requiring appropriate approvals for request to establish accounts;

e. Establishing, activating, modifying, disabling, and removing accounts;

f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;

g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;

h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;

i. Granting access to the system based n: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associate missions/business functions; and

j. Reviewing account [Assignment: organization-defined frequency]."

Additionally, Separation of Duties (AC-5) states:

"The organization:

a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;

b. Documents separation of duties; and

c. Implements separation of duties through assigned information system access authorizations.

Supplemental Guidance: Examples of separation of duties include (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles."

Cause/Effect:

Based on a consideration of priorities and limited resources, Fund management has not yet allocated the resources required to develop and implement segregation of duties controls that mitigate the risks associated with the condition including, but not limited to, segregating system administration roles and access review performer roles among different individuals.

Historically, the individual responsible for performing and signing off on the BARTS periodic review of access has also been the application owner and primary security administrator for the BARTS application. The primary security administrator role for the application has been transitioned to OIT within the last year, and management is currently developing the transition plan to revoke the access to administer security from the individual responsible for performing the periodic review of access.

By not segregating the responsibility for performing the periodic review of access for the application from those who procedurally administer access to BARTS, the potential exists that unauthorized access changes within BARTS user accounts go unnoticed.

Recommendations:

We recommend that Fund management:

- Develop and formally document procedures for performing reviews that address and evaluate the appropriateness of the individuals performing the review, verify their ability to determine the appropriateness of access for each user, and ensure that the reviewers do not have additional responsibilities that will result in a lack of segregation of duties.

- Periodically monitor control performer adherence to these control activities.

Management's Response:

Management concurs with the facts of this finding. The BPC chief (who validates authorized staff) was not available (on-site) during the documentation period and hence was not available to sign the review document. The review however was a collaborative effort between the system owner and OIT.

8. DOCS Access to Programs and Data – DOCS Wage Modification Access

Condition:

We noted that 29 out of 42 users with the ability to add or modify wage information per their system access rights within the DOCS application tested did not require this level of access in accordance with their job responsibilities.

Criteria:

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996, Section 3.12, states:

"Organizations should base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions."

Cause/Effect:

Fund management has currently not configured access for the DOCS application in a manner that is granular enough to restrict access to perform this function to those who require it in accordance with their job responsibilities.

As a result, there is an increased risk that the users referenced in the condition above could apply changes to client wage information within the DOCS application that inappropriately influences monetary eligibility for unemployment benefits payments.

Management has indicated that there were no known cases in which this access was utilized to make unauthorized wage changes within the application.

Recommendations:

We recommend that Fund management refine access restrictions over the ability to update wage information within DOCS to restrict access based on principles of least privilege including restricting to read-only in production access those IT personnel who are responsible for advanced troubleshooting within the application.

However, if system limitations prevent this from being implemented in a feasible manner, we recommend that Fund management implement an independently-operated monitoring control over changes to wage information within the DOCS application. This review should be:

- Performed at a frequency determined by management (monthly or quarterly);
- Performed by someone with knowledge of the changes, who does individually have access to make the changes within the system;
- Based on system-generated reports of wage changes within the applications; and,
- Formally documented and signed by the reviewer.

Management's Response:

Management concurs with the facts of the finding. Management is already exploring the best methodology to implement the proposed granularity of access controls.

9. Computer Operations for BARTS – BARTS Backup Tape Recovery and Restoration

Condition:

During FY 2012, Fund management did not perform official testing to confirm that the backup tapes related to BARTS can be successfully recovered and restored.

Criteria:

NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, May 2010, states under *3.4.1 Backup and Recovery and 3.5.1 Testing:*

3.4.1 Backup and Recovery

"Backup and recovery methods and strategies are a means to restore system operations quickly and effectively following a service disruption. The methods and strategies should address disruption impacts and allowable downtimes identified in the Business Impact Analysis (BIA) and should be integrated into the system architecture during the Development/Acquisition phase of the System Development Life Cycle (SDLC). A wide variety of recovery approaches may be considered, with the appropriate choice being highly dependent upon the incident, type of system, BIA/Federal Information Processing Standards (FIPS) 199 impact level, and the system's operational requirements.22 Specific recovery methods further described in Section 3.4.2 should be considered and may include commercial contracts with alternate site vendors, reciprocal agreements with internal or external organizations, and service-level agreements (SLAs) with equipment vendors. In addition, technologies such as redundant arrays of independent disks (RAID), automatic failover, uninterruptible power supplies (UPS), server clustering, and mirrored systems should be considered when developing a system recovery strategy.

Several alternative approaches should be considered when developing and comparing strategies, including cost, maximum downtimes, security, recovery priorities, and integration with larger, organization-level contingency plans. Table is an example that can assist in identifying the linkage of FIPS 199 impact level for the availability security objective, recovery priority, backup, and recovery strategy."

3.5.1 Testing

"Information System Contingency Plan (ISCP) testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing can take on several forms and accomplish several objectives but should be conducted in as close to an operating environment as possible. Each information system component should be tested to confirm the accuracy of individual recovery procedures. The following areas should be addressed in a contingency plan test, as applicable:

- Notification procedures;
- System recovery on an alternate platform from backup media;
- Internal and external connectivity;
- System performance using alternate equipment;
- Restoration of normal operations; and
- Other plan testing (where coordination is identified, i.e., Continuity of Operations Plan (COOP), Business Continuity Plan (BCP))"

Cause/Effect:

Due to lack of incidents and failures requiring data recovery for BARTS during FY 2012, there was no need to recover and restore information from backup tapes. Additionally, management has not implemented formal policies and procedures to document recovery and restoration exercises to confirm that the backup tapes related to BARTS can be successfully recovered and restored.

As a result, a lack of implementing formalized testing procedures to confirm the recoverability of the backup tapes increases the risk that vital computer records and data on the backup tapes may not be recovered successfully in case of failure for continuity of operations purposes.

Recommendation:

We recommend that Fund management implement policies and procedures, including training of personnel, to ensure that backup tapes are officially tested on a semi-annual basis to confirm successful recovery and restoration of data.

Management's Response:

Management concurs with the facts of this finding. Restoring backups from tape involves coordination between DOES and OCTO (the consolidated datacenter). OIT will review its operations and come up with a streamlined procedure that will afford such testing. It should however be noted, that any plan put in place has a dependency on the data host (OCTO) who plays a major role towards a successful outcome.

10. Incorrect Underlying Data Used to Estimate Claimants Payable

Condition:

DOES management estimates claimants payable at fiscal year end. The estimate is broken into two categories of claimants: (1) first-time claimants that have been found eligible within 20 days of the fiscal year end as of September 30, 2012 and (2) first-time claimants who began receiving benefits between April and September 2012 that will continue to collect benefits after the fiscal year end. During our testwork, we noted that the average weekly benefit calculated by management was $297. We recalculated the average weekly benefit to be $292.45. Furthermore, we noted that the population of first-time claimants found eligible 20 days prior to the fiscal year end per management was 1,216 claimants. KPMG determined through supporting documentation that first-time claimants found eligible within the last 20 days of the fiscal year was 1,224. These differences led to an overstatement of claimants payable of $741,936.

Criteria:

Governmental Accounting Standards Board (GASB) Statement No. 1, *Objectives of Financial Reporting*, recognizes the basic characteristics of financial reporting objectives as understandability, reliability, relevance, timeliness, consistency, and comparability. While GASB does not identify specific control standards, state and local governments follow internal control guidance to meet those objectives. Two of the major sources of guidance for state and local governmental units on auditing and reporting on internal control are the Single Audit Act and Government Auditing Standards (GAS), also known as generally accepted government auditing standards (GAGAS), and popularly known as the Yellow Book. These standards are produced by the Government Accountability Office (GAO). GAO's Standards for Internal Control states that for an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout an agency to achieve all of its objectives. These standard control activities help to ensure that all transactions are completely and accurately recorded.

Yellow Book, Appendix I, section A1.08 d., states that management at a State and Local government entity is responsible for *"establishing and maintaining effective internal control to help ensure that appropriate goals and objectives are met; following laws and regulations; and ensuring that management and financial information is reliable and properly reported."*

Per the Committee of Sponsoring Organizations (COSO) Volume II Guidance on Monitoring Internal Control Systems, internal controls *"ensure that necessary actions are taken to address risks to achieving objectives. Control activities occur throughout the organization, at all levels, and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties."*
Cause/Effect:

The above conditions resulted from ineffective management review of the estimate's supporting documentation when reviewing the journal entry. As a result, claimants payable is misstated.

Recommendation:

We recommend that Fund management should adopt a review process that ensures that underlying data for an estimate is complete and accurate prior to recording the journal entry.

Management's Response:

Management concurs with the facts of this finding.

11. Allowance for Doubtful Accounts Non-GAAP Policy – Tax Claimants Receivable

Condition:

When an accounting policy does not exist at a specific agency, the agency utilizes the District's policy to formulate a methodology. Therefore, DOES management utilizes a DC policy that is not within the bounds of Generally Accepted Accounting Principles (GAAP). The District's policy only allows DOES to estimate their allowance for doubtful accounts for any claimants receivable accounts that are 451 days or older and for any employer taxes receivable accounts that are older than 2 years.

Criteria:

GAAP states that bad debt be recognized and deducted from revenue during the same time period the revenue is generated. Three GAAP methodologies for estimating the allowance for bad debts are:

1. Percentage of Credit Sales Method;
2. Aging of Accounts Receivable method; and
3. Percentage of Ending Accounts Receivable method.

According to GASB 33, paragraph 16, "Revenues should be recognized, net of estimated refunds and estimated uncollectible amounts, in the same period that the assets are recognized, provided that the underlying exchange transaction has occurred."

Cause/Effect:

The above condition resulted from DOES management only being allowed to use the District's policy, which utilizes Non-GAAP methods to estimate the allowance for doubtful accounts. As a result, net accounts receivable may be materially misstated as the collectability of receivables is not considered for bad debts could have a material impact on the financial statements of the Fund.

Recommendation:

We recommend that Fund management adopt a policy for estimating the allowance for doubtful accounts in accordance with GAAP.

Management's Response:

Management concurs with the facts of this finding.