GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL

DISTRICT OF COLUMBIA
UNEMPLOYMENT COMPENSATION FUND

Management Letter Report
Years Ended September 30, 2013, and 2012

CHARLES J. WILLOUGHBY
INSPECTOR GENERAL

OIG No. 14-1-10BH(a) May 19, 2014

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

May 19, 2014

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) 2013, KPMG LLP (KPMG) submitted the enclosed final management letter report on the District of Columbia Unemployment Compensation Fund (Fund) for years ended September 30, 2013, and 2012 (OIG No. 14-1-10BH(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 weaknesses in general information technology controls. Management responses for three of the eight reported findings and recommendations with which management does not concur are included in Attachment A immediately following the recommendations.

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

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)
Mr. Jeffrey DeWitt, Chief Financial Officer, Office of the 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)
Mr. Lawrence Perry, Deputy 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: Mark Stephenson (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: Chris Barkley (via email)
The Honorable Mark Begich, Chairman, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia, Attention: Jason Smith (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: Angela Ohm (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: Angela Ohm (via email)

The Honorable Barbara Mikulski, Chairwoman, Senate Committee on Appropriations, Attention: Kali Matalon (via email)
The Honorable Richard Shelby, Ranking Member, Senate Committee on Appropriations, Attention: Dana Wade (via email)
The Honorable Tom Udall, 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

March 20, 2014

Inspector General of the Government of the District of Columbia,
Director of the Department of Employment Services, and
The Government of the District of Columbia

Unemployment Compensation Fund
Washington, DC

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of the Unemployment Compensation Fund (the Fund), as of and for the year ended September 30, 2013 and 2012, 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 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 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.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Fund’s organization gained during our work to make comments and suggestions that we hope will be useful to you.

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

The Fund’s written response to our comments and recommendations has not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

This communication is intended solely for the information and use of management, the Inspector General, the Director of DOES, others within the organization, and the Government of the District of Columbia, 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

Weaknesses in the Fund's General Information Technology Controls

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 key control areas: (1) Access to Programs and Data (APD), (2) Program Changes (PC), (3) Program Development, and (4) Computer Operations. The internal control criteria utilized during our testing of GITCs including the following:

- National Institute of Standards and Technology (NIST) *Special Publication 800-53, Revision 3*, Sections PE-2, AC-5, AC-2, IA-5, AC-7, AC-6;
- NIST S*pecial Publication 800-14*, Section 3.12;
- NIST *Special Publication 800-12*;
- NIST *Special Publication 800-64;* and
- DOES OIT *User Account and Password Management Standard, Access Control Policy, and Change Control Policy*.

During our fiscal year (FY) 2013 audit, the following findings were identified.

General Information Technology Controls:

1. APD - Data Center Physical Access

During FY2012 testing over the physical access controls for the Office of the Chief Technology Officer (OCTO) Data Center 1 (ODC1), it was noted that 133 individuals held badge access to the server room for a portion of FY2012 when it was not required to effectively complete 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, none of these individuals required this level of access.
- 120 individuals were members of other agencies that were granted access to the data center without the consultation of OCTO management.

In April 2013, management began a recertification of badge access to ODC1 and requested removal for all individuals that no longer required access to the facility including all personnel outside of OCTO. However, the badge access removal was not processed by the Protective Services Division (PSD) for 10 of these individuals until September 25, 2013. As such, these individuals had inappropriate access for most of FY2013 and, although remediated at the end of FY2013, a deficiency in the control environment existed until this time.

The administration of physical access to the ODC1 server room is managed by agencies outside of OCTO's purview, and as such, OCTO had 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.

If individuals obtain/retain inappropriate physical access to networking devices, operating consoles, host computers and peripherals located in the data center there is an increased risk that this equipment could be damaged, removed, or accessed through a variety of techniques to obtain and use unauthorized system privileges, thereby impacting hosted applications' availability and/or operational integrity.

Recommendation:
We recommend that OCTO 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 new badge access provisioning, badge access termination, and badge access periodic review procedures.

When taking ownership of physical access administration for ODC1, management should ensure that the following control activities are implemented 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 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 ODC1 management personnel with appropriate knowledge of those who require this level of access.

In line with these above recommendations, control performers should be trained on these processes, and management should monitor adherence to these control activities going-forward.

Management Response:
Management concurred with the facts of this finding.

2. <u>APD - District Online Compensation System (DOCS), District Unemployment Tax Administration System (DUTAS), and Budget and Reporting Tracking System (BARTS) Application Administrator Access</u>

Within FY2012 testing, the following control deficiencies were noted within the access administration for DOCS, DUTAS, and BARTS:

- Two of the DUTAS and one of the DOCS application security administrators possessed conflicting responsibilities as either developers or business end users who had access to administer security for the applications. Specifically, it was noted that one developer and one business user had access to administer security for DUTAS and one business user had the ability to administer security for DOCS. While management had deemed their access appropriate to perform these functions, the lack of segregation of duties between these functions represented a weakness in the internal control environment for these two applications.

- The BARTS user access review completed on June 6, 2012 was performed by a user who had the logical access rights required to administer security for BARTS. This combination of responsibilities within the access review process represents a segregation of duties conflict.

Upon review in August 2013, it was determined that:

- The DOCS application security administrator and two of the three DUTAS administrators noted in the finding above retained access to these functions and their conflicting responsibilities. While management has deemed their access appropriate to perform these functions, the lack of segregation of duties between these functions coupled with the fact that a compensating control to mitigate the risk associated with this specific condition has not been designed and implemented by management represents a weakness in the internal control environment for these two applications.
- The periodic access reviews for BARTS and DUTAS were completed by individuals who have security administrator privileges within their respective applications. Although this access has been deemed appropriate by management, this combination of responsibilities within the access review process represents a segregation of duties conflict for which a compensating control to mitigate the risk associated with this specific condition has not been designed and implemented by management.

Therefore, these control deficiencies have not been remediated from FY2012.

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 developer noted with access to administer security to DUTAS is one of the two Office of Information Technology (OIT) personnel currently aligned to support the DUTAS system. 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 FY2012, management moved the primary security administrator role for DOCS out of UI into the 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.

Historically, the individual responsible for performing and signing off on the BARTS and DUTAS periodic review of access has also been the application owner and primary security administrator for the BARTS and DUTAS applications. The primary security administrator role for the applications has been transitioned to the OIT, 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.

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. Such individuals may have access to bypass certain system or process-based controls within the applicable business processes.

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 unauthorized or otherwise inappropriate access to privileges in DOCS and DUTAS.

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

However, in performing testing over the access provisioning and termination processes for applications noted in the condition above, no cases were identified in which access rights were granted by individuals with security administration capability in an unauthorized manner.

Recommendation:
We recommend that 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.

In addition, it is recommended that 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
- 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.

Additionally, we recommend that management periodically monitor control performer adherence to these control activities.

Management Response:
Management concurred with the facts of this finding.

3. <u>APD - DOCS Wage Modification Access</u>

Within FY2012 testing, it was determined that 29 of 42 users had the ability to add or modify wage information per their system access rights within the DOCS application when it was not required to fulfill their job responsibilities.

Upon review in August 2013, it was determined that there were 41 users with access to update wages and 25 of the 29 users noted as inappropriate in FY2012 continued to possess access to this function. In addition, it was determined that all individuals with access to modify wages also have access to modify eligibility parameters. While management deems all individuals with access to modify eligibility parameters appropriate, the pairing of this access with access to modify wage information represents a combination of incompatible duties and coupled with the fact that a compensating control to mitigate the risk associated with this specific condition has not been designed and implemented by management represents a weakness in the internal control environment. Therefore, this finding has not been remediated from FY2012.

Historically, system limitations have prevented management from configuring access within DOCS to separate access privileges required to modify eligibility parameters and wage data. During FY2013, management was in the process of re-configuring the application to address this limitation so that privileges enabling the modification eligibility parameters could be assigned separately from privileges enabling the modification of wage information. However, the process not completed prior to the end of FY2013.

As a result of this finding, 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.

Recommendation:
We recommend that management restrict DOCS access to update wage information based on principles of least privilege, including:

- Configuring read-only access for IT personnel responsible for advanced application troubleshooting and,
- Separating the assignment of wage update and the eligibility modification privileges to different business users.

However, if system limitations prevent this from being implemented in a feasible manner, it is recommended that management implement and independently-operating monitoring control over changes to wage information within the DOCS application. This review should be:

- Performed at a controlled frequency determined by management (monthly or quarterly);
- Performed by an independent party with knowledge of the changes, who does not individually has access to make the changes within the system;
- Based on system-generated reports of wage changes within the application; and,
- Formally documented and signed by the reviewer.

Management Response:
Management concurred with the facts of this finding.

4. <u>APD - DOCS and WEBBS Password Settings</u>

During access control testing for DOCS and the web interface, WEBBS, it was noted that the application level password configurations did not comply with requirements set forth in the Department of Employment Services (DOES) password policies (i.e., the DC DOES OIT User Account and Password Management Standard). Specifically, the minimum password length was set to five characters (whereas policy require the setting be between 6 and 8 characters), and required settings for password complexity, password expiration, and account lockout after unsuccessful log-in attempts were not enforced.

Although access to the DOCS and WEBBS applications require the user to separately authenticate, using a password upon which strong settings are enforced through the DOES network and/or the Resource Access Control Facility (RACF) on the mainframe before logging into DOCS and WEBBS applications, the lack of alignment between the DOES password policies and the DOCS and WEBBS password configuration represents a weakness in the control environment.

Due to system limitations, upon implementation of DOCS and WEBBS, the password parameters were not set in accordance with the current DOES Password Management Policy for password-based authentication. Subsequently, due to resource limitations and efforts required, the password parameters have not been updated since implementation to reflect the current password policy requirements.

Weakly configured password settings increase the risk that unauthorized users could access sensitive system functions, which could negatively impact the confidentiality, integrity and availability of application data.

Recommendation:
We recommend that management enforce strong password settings in accordance with the DC DOES OIT User Account and Password Management Standard in remediation of the finding above.

Management Response:
Management did not concur with the facts of this finding. Management stated that, “DOCS/WEBB currently has a system limitation of four character password. By way of architecture, changes to such programming would result in major disruption of access to the system. This is not acceptable to critical unemployment insurance business operations.

Current mitigating steps include:
1. Three level authentication. DOES DOCS users need to first login to the network domain, and then login to the mainframe before getting to DOCS application. The Domain and Mainframe authentication meets passwords policy standards.
2. DOES reviews access to DOCS and WEBBS periodically

Strategic Planning
1. Authentication standards and overall security best practices are parameters on discussion points towards VI system modernization.”

5. <u>APD - New User Access Authorization Forms – DUTAS</u>

During FY2012 testing, it was determined that for one of three users granted access to DUTAS application selected for testing during the fiscal year, there was no notation on the access request form submitted for the user indicating specific roles or level of access to DUTAS that was authorized by management.

During FY2013 testing, it was determined that, for one out of three new users granted access to DUTAS selected for testing during the fiscal year, the access granted to DUTAS did not align with the access rights explicitly requested and approved on the access request form. While it was determined that the access rights assigned were appropriate for the user, this lack of documentation represents a control activity weakness in the new user provisioning process, and therefore, the finding has not been remediated from FY2012.

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 the 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 was considered appropriate. Management believed that these undocumented methods of determining the access levels would be sufficient to address the risk that inappropriate or unnecessary access would be granted to DUTAS

While the access rights assigned to the user identified in the condition above were determined to be appropriate, thus 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, there is a potential for users possessing conflicting privileges causing lack of segregation of duties and inappropriate access to information systems resources. These users could advertently or inadvertently use various functions to process transactions or change data within the system that is not authorized or that compromises the integrity of the application and its data.

Recommendation:
We recommend that management re-emphasize the established process for granting new user access to DUTAS, which requires a formal documentation and approval of the specific access that should be granted to new DUTAS users. In doing so, management should consider formally documenting the mapping between the user roles or menu paths that can be requested on the access request form for DUTAS to the specific screens that are to be provisioned based on these requests. Additionally, management should periodically monitor control performer adherence to these control activities.

Management Response:
Management concurred with the facts of this finding.

6. <u>APD - BARTS Operating System, Database Administrative Access, and Database password configurations</u>

During FY2012 testing, the accounts with operating system and database administrative privileges supporting BARTS were reviewed and the following conditions were noted:

1) Eight system and generic accounts with active access to administer the operating system no longer required these administrative privileges. Per inquiry of management, knowledge of the passwords to these accounts has been restricted to the same group of authorized operating system administrators, who also possess access to these privileges through their own unique accounts. However, the active access for the generic accounts, which is no longer necessary, represents a weakness in the control environment.

2) Access to the "sa" generic account, which possesses database administrative privileges, is shared by three individuals in addition to their unique accounts. Although, per inquiry of management, these three individuals are appropriate to possess access to database administrative privileges, there had not been additional compensating controls such as rotating the password in a controlled and periodic manner to mitigate the risk from sharing a generic account. Additionally, eight individuals with Domain Administrator privileges have access to administer the database supporting the BARTS application through the BUILTIN\Administrators conduit. The access of these individuals to administer the database, which was not commensurate with their job responsibilities, represented a weakness in the control environment.

Upon review in August 2013, it was determined that the eight system and generic accounts with active access to administer the operating system that no longer required these privileges in FY2012 remained active in FY2013, and as a result, this portion of the finding was not remediated during FY2013.

In addition, at the database level, it was determined that to address the risk associated with inappropriate access to the database through either the “sa” generic account or other unique accounts, management has implemented a semi-annual periodic review over the actions taken by reviewing the event viewer logs. However, the review does not explicitly outline the follow-up and the analysis of the activity of the “sa” account, nor does it include a verification to identify operating system accounts that no longer require administrative access privileges. As a result, the deficiencies identified in FY2012 have not been remediated. Additionally, it was further noted that, due to limitations associated with use of Windows SQL Server 2000 as the BARTS database management system, password complexity could not be enforced for the "sa" generic account.

Due to system limitation and lack of resources, 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 disabled or deleted timely. Additionally, due to system limitation, management cannot enforce system password complexity at the database level.

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 that are not monitored or reviewed, and account login information and related accounts could be accessed and used in an unauthorized manner.

Provisioning database administration privileges to users who neither require them nor possess requisite knowledge for their use increase the risk that inadvertent changes are made to the database environment that adversely impact the integrity of the system and/or financial data.

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

- A periodic review of all accounts with access to administer the operating system and database, which verifies the appropriateness of both generic and unique accounts, including those assigned privileged access through conduit accounts (e.g. BUILTIN\Administrators). As a result, all inappropriate accounts should be removed. This review should be:
  - Performed at a regular frequency determined by management (monthly or quarterly)
  - Performed by an independent party with knowledge of the appropriate administrators, who does not individually have administrator access to make changes within the system
  - Based on system-generated reports of administrators listings; and
  - Formally documented and signed by the reviewer.
- A defined process for periodically changing the "sa" account password, such that password changes are performed at a regular frequency, incident management system work tickets are prepared to document change requests and completion, and knowledge of the password is restricted only to those individuals who require access to the “sa: account to perform job responsibilities.
- A periodic review of operating system activity that explicitly outlines requirements for completing the analysis of the activity of the “sa” account, what constitutes suspicious activity, and requirements for researching and following up on such activity. This review should be:
  - Performed at a regular frequency determined by management (monthly or quarterly)
  - Performed by an independent party with knowledge of the operating system, who does not individually have administrator access to the operating system
  - Based on system-generated reports of operating system activity; and
  - Formally documented and signed by the reviewer.

These requirements should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, we recommend that management monitor control performer adherence to the procedure on a periodic basis.

Management Response:
Management concurred with the facts of this finding.

7. APD and PC - DUTAS Access to Migrate Changes and Database Administration Segregation of Duties

Within FY2012 testing, it was determined that the following deficiencies existed:

1) Three DOES personnel and 11 OCTO personnel for the DOCS application had access to DOCS production datasets that was not commensurate with job responsibilities. In addition, five OCTO systems programmers for the DUTAS application had access to DUTAS datasets that was not commensurate with their job responsibilities.
2) One individual with development responsibilities had access to migrate changes to production for the DOCS and DUTAS applications through access to the load library using the employee's own login ID to the system. This user also had access to modify the backend data for the DOCS and DUTAS applications.

In August 2013, the levels of access above were reviewed, and it was determined that deficiency 1) above was remediated. Regarding deficiency 2) above, it was determined that the one individual noted with development responsibilities continued to possess access to migrate changes to production and modify backend data for DUTAS using the employee's own login ID. While management has deemed this individual's access appropriate to perform this function, the lack of segregation of duties between these functions coupled with the fact that a compensating control to mitigate the risk associated with this specific condition has not been designed and implemented by management represents a weakness in the internal control environment for DUTAS. As a result, this finding has not been fully remediated from FY2012.

Based on a consideration of priorities and limited resources, management had not allocated the resources required to develop and implement segregation of duties controls that mitigate the risks associated with deficiency 2), including, but not limited to, the segregation of program development roles from the production application and database administration roles among different individuals and/or other mitigating controls such as monitoring the activities of the individuals with administrative level access. Additionally, in the process of implementing change management controls to mitigate the risk associated developers possessing access to migrate changes to production, management believed it necessary to allow the individual noted above the access rights to migrate changes to production for DUTAS. In doing so, management was aware that this individual would possess these conflicting responsibilities, which management deemed necessary to support the consistent operations of the application until these change management controls were stabilized.

The lack of segregation of duties controls increases the risk that developers can potentially 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 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 potentially 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.

Recommendation:
We recommend that management develop and implement processes and controls associated with the DUTAS change management function that establish one or more of the following:

- Organizational and logical segregation of program development roles from production system and database administration roles among different individuals; and/or,
- Implementation of one or more independently operated monitoring controls over the activities of the developer (and other individuals) with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system. This review should be:
    - Performed at a controlled frequency determined by management (monthly or quarterly);
    - Performed by an independent party with knowledge of the changes, who does not individually have access to make changes within the system;
    - Based on system-generated reports of changes within the application; and
    - Formally documented and signed by the reviewer.

Further, we recommend that management monitor the effectiveness of these controls on a regular and periodic basis.

Management Response:
Management did not concur with the facts of this finding. Management stated that, "The user in question was responsible for OIT application development work that required access to UI Datasets. His role was being transitioned to other support resources. However, it was deemed necessary to retain user as a backup till management was comfortable with the transition. This was a strategic plan and user's access was completely removed based on internally discussed time lines."

8. PC - Program Change Controls for DUTAS

During FY2012 testing, it was determined that for one of three modules changed during FY2012, the corresponding change was not reflected within the manual listing that is used for tracking program changes for DUTAS. In addition, documentation that supported the testing and approval of this specific change was not available.

Upon review in FY2013, it was determined that five of 15 module changes selected for testing were not formally documented within a change management ticket, and therefore did not have corresponding testing and approval evidence documented. Additionally, two other changes were documented in a change management ticket, but did not have supporting documentation for approval and testing available. While it was determined that all of the changes in question were appropriate and some of the changes represented minor changes not impacting system functionality, this lack of documentation represents a weakness in the program change management process that has not been remediated from FY2012.

DUTAS currently does not have an automated change tracking tool interfacing directly with the system and/or an ability to track systematically all changes within an internal database. Therefore, a manual process exists. The manual process for tracking program changes for DUTAS in the change control log and retaining documentation of testing and approving of the change was not followed for the program changes noted within the condition above. This was due to management and control performer oversight in retaining the supporting documentation as evidence of testing and approving.

The use of a manual change control log rather than an automated process and tool for DUTAS program changes makes it difficult to maintain a systematic log of program changes and enforce proper review and approvals through change stage gates with audit trails.

Without consistently following the formally documented change management process, there is an increased risk that unauthorized and/or unintended program changes potentially may be implemented into the production environment. This could result in a loss of confidentiality, integrity, and availability of the system and data. However, for each of the cases noted in the observation above, management indicated that the change was appropriate. The changes did not have the potential to impact the confidentiality, integrity, and/or availability of the data within DUTAS.

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

- Management should re-emphasize the established process for tracking, testing, and approving program changes to the DUTAS application production environment with all parties responsible for control performance. This should increase the consistency with which the process is followed. The manual log should be consistently updated for every change applied to the production environment, including minor changes not impacting system functionality, and it should capture the load library modules impacted by the change. Additionally, management should periodically monitor control performer adherence to these control activities.
- Management should investigate opportunities to migrate to a more automated process to track changes and change control documentation for DUTAS. This may include leveraging software or tools to request, document, and approve program changes.

Management Response:
Management did not concur with the facts of this finding. Management stated that, “The purpose and intent of the OIT change management policy/process is for authorizing, testing and documenting changes that potentially can impact information systems in a manner that can adversely affect availability, integrity and confidentially of the data contained therein. The five program changes in question were deemed appropriate and they cause no harm to the system

and/or data contained therein. Testing documentation would not have made these "types" of changes less harmful and hence, pose an insignificant risk to DUTAS.

Documentation of these types of changes will be emphasized and communicated to the developer. It should however be noted that all other changes that potentially could have impacted the system adversely, went through the proper change management documentation and testing process and therefore, the notion of a weakness within the change management process is not clear.”