

DISTRICT OF COLUMBIA OFFICE OF THE INSPECTOR GENERAL

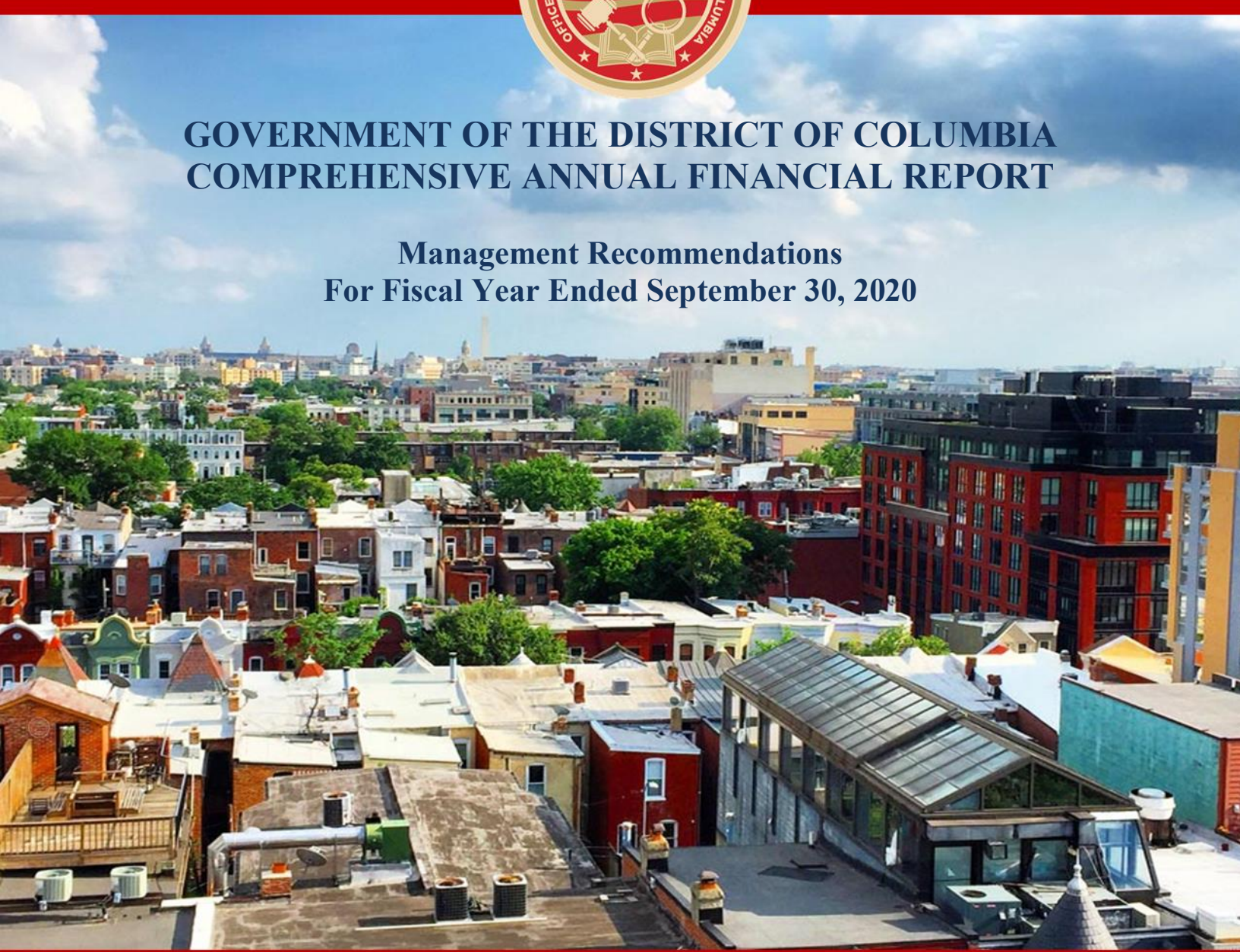
OIG Project No. 21-1-03MA(a)

January 2021



GOVERNMENT OF THE DISTRICT OF COLUMBIA COMPREHENSIVE ANNUAL FINANCIAL REPORT

**Management Recommendations
For Fiscal Year Ended September 30, 2020**



Guiding Principles

*Workforce Engagement * Stakeholders Engagement * Process-oriented * Innovation
* Accountability * Professionalism * Objectivity and Independence * Communication * Collaboration
* Diversity * Measurement * Continuous Improvement*

Mission

Our mission is to independently audit, inspect, and investigate matters pertaining to the District of Columbia government in order to:

- prevent and detect corruption, mismanagement, waste, fraud, and abuse;
- promote economy, efficiency, effectiveness, and accountability;
- inform stakeholders about issues relating to District programs and operations; and
- recommend and track the implementation of corrective actions.

Vision

Our vision is to be a world-class Office of the Inspector General that is customer-focused and sets the standard for oversight excellence!

Core Values

Excellence * Integrity * Respect * Creativity * Ownership
* Transparency * Empowerment * Courage * Passion
* Leadership



GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



January 29, 2021

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

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

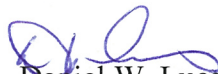
Dear Mayor Bowser and Chairman Mendelson:

Enclosed is the final report entitled *District of Columbia Management Recommendations* report for fiscal year (FY) 2020 (OIG No. 21-1-03MA(a)) by McConnell Jones, LLP (MJ) issued January 28, 2021. MJ submitted this report as part of our overall contract for the audit of the District of Columbia's general-purpose financial statements for FY 2020.

This report sets forth MJ's comments and recommendations intended to improve the effectiveness of internal controls over the District operations and programs. When addressed, these improvements can increase assurances that District agencies run their operations efficiently and effectively, report reliable information about their operations, and comply with applicable laws and regulations. The report also includes MJ's summary of prior year management recommendations and the corresponding implementation status.

If you have questions about this report, please contact me or Fekede Gindaba, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,


Daniel W. Lucas
Inspector General

DWL/ws

Enclosure

cc: See Distribution List

DISTRIBUTION:

Mr. Kevin Donahue, City Administrator for the District of Columbia, Office of the City Administrator (via email)
Mr. Barry Kreiswirth, General Counsel, Office of the City Administrator, District of Columbia (via email)
Mr. Jay Melder, Assistant City Administrator, Office of the City Administrator, District of Columbia (via email)
Mr. Eugene Adams, Director, Mayor's Office of Legal Counsel (via email)
Mr. John Falcicchio, Deputy Mayor for Planning and Economic Development and Chief of Staff, Executive Office of the Mayor (via email)
The Honorable Kenyan R. McDuffie, Chair Pro Tempore, Council of the District of Columbia (via email)
The Honorable Anita Bonds, At-Large Councilmember, Council of the District of Columbia (via email)
The Honorable Christina Henderson, At-Large Councilmember, Council of the District of Columbia (via email)
The Honorable Elissa Silverman, At-Large Councilmember, Council of the District of Columbia (via email)
The Honorable Robert C. White, Jr., At-Large Councilmember, Council of the District of Columbia (via email)
The Honorable Brianne K. Nadeau, Ward 1 Councilmember, Council of the District of Columbia (via email)
The Honorable Brooke Pinto, Ward 2 Councilmember, Council of the District of Columbia (via email)
The Honorable Mary M. Cheh, Ward 3 Councilmember, Council of the District of Columbia (via email)
The Honorable Janeese Lewis George, Ward 4 Councilmember, Council of the District of Columbia (via email)
The Honorable Charles Allen, Ward 6 Councilmember, Council of the District of Columbia (via email)
The Honorable Vincent C. Gray, Ward 7 Councilmember, Council of the District of Columbia (via email)
The Honorable Trayon White, Sr., Ward 8 Councilmember, Council of the District of Columbia (via email)
Ms. LaToya Foster, Director of Communications, Office of Communications, Executive Office of the Mayor (via email)
Ms. Jennifer Reed, Director, Office of Budget and Performance Management, Office of the City Administrator (via email)
Ms. Nyasha Smith, Secretary to the Council (via email)
The Honorable Karl Racine, Attorney General for the District of Columbia (via email)
Mr. Jeffrey DeWitt, Chief Financial Officer, Office of the Chief Financial Officer (via email)
Mr. Timothy Barry, Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
The Honorable Kathy Patterson, D.C. Auditor, Office of the D.C. Auditor, Attention: Cathy Patten (via email)
Mr. Jed Ross, Director and Chief Risk Officer, Office of Risk Management (via email)
Mr. Wayne McConnell, Managing Partner, McConnell & Jones LLP (via email)

**GOVERNMENT OF THE
DISTRICT OF COLUMBIA**

MANAGEMENT RECOMMENDATIONS

FOR THE YEAR ENDED SEPTEMBER 30, 2020

TABLE OF CONTENTS

I CURRENT YEAR FINDINGS

2020-1	Frequency of Payroll Clean-up Process	1
2020-2	Lack of Approval on Notification of Personnel Action Forms	2
2020-3	Controls over Compliance with the Quick Payment Act of 1984 Were Not Operating Effectively	3
2020-4	Controls Over Authenticator Management Password-based Authentication Were Not Operating Effectively	4
2020-5	Controls Over Reviews of Information Security Policies and Procedures Were Not Operating Effectively	5
2020-6	Controls Over Least Privilege Review of User Privileges Were Not Operating Effectively	7
2020-7	Controls Provide Reasonable Assurance That Employees Receive Proper Security Awareness Training	8
2020-8	Controls Over Reviews of Information Security Policies and Procedures Were Not Operating Effectively	9
2020-9	Controls Over Terminated User Access Are Ineffective	11
2020-10	Controls Over Security Awareness Training and Policy Acknowledgment Procedures Were Not Operating Effectively	12
2020-11	Controls Over Emergency Procurement Were Not Operating Effectively	13

II PRIOR YEAR FINDINGS

Status of Prior Year Findings and Recommendations	18
---	----



To the Mayor, Members of the Council of the District of Columbia,
Inspector General of the District of Columbia and
Chief Financial Officer of the District of Columbia

In planning and performing our audit of the basic financial statements of the Government of the District of Columbia and related entities (the District) as of and for the year ended September 30, 2020, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, we considered the District's internal controls over financial reporting (internal controls) as a basis for designing audit procedures that were appropriate in the circumstances 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 District's internal controls. Accordingly, we did not express an opinion on the effectiveness of the District's internal controls over financial reporting.

Our consideration of internal controls was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal controls that might be significant deficiencies or material weaknesses, and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified. Although no matter of a material weakness was noted, other recommendations have been noted which we believe will further improve the District's internal controls or operating effectiveness.

A *deficiency* in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A *material weakness* is a deficiency or combination of deficiencies in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

This letter does not affect our report dated January 28, 2021, on the financial statements of the District. Our comments and recommendations, which have been discussed with appropriate members of management, are intended to improve the internal controls or result in other operating improvements.

This report is intended solely for the information and use of the management, others within the organization, the Mayor and Members of the Council of the District of Columbia, the Inspector General of the District of Columbia and the Chief Financial Officer of the District of Columbia, and is not to be and should not be used by anyone other than these specified parties. We will be pleased to discuss these comments with you and, if desired, to assist you in implementing any of the suggestions.

Washington, D.C.
January 28, 2021

I. CURRENT YEAR FINDINGS

District of Columbia Public Schools (DCPS)

Finding 2020-1. Frequency of Payroll Clean-up Process

The payroll clean-up process at DCPS is not occurring at the appropriate interval to prevent the District from incurring additional fringe benefit expenses for employees who are no longer with the agency.

Per District policies, documentation must be provided to support the termination (letter of resignation or Not-To-Exceed (NTE) Offer letter) of a District or DCPS employee. DCPS has a business rule that if an individual does not report for work or log time into the system for 3 months, they are to consider the employee to have abandoned the job.

As part of our review, we noted instances where the appropriate termination documentation was unavailable for review. We did note a remark in the Notification of Personnel Action forms (“SF-50”) stating, “termination due to payroll clean-up”. As a result of that notation, additional information was obtained from the agency that showed that the payroll clean-up process occurs twice a year and employees remained in the system for a period of time after they had abandoned their jobs. McConnell & Jones LLP (MJ) selected 60 samples for the payroll terminations, which included 28 selections from DCPS. We noted that two of the samples had a termination date on the SF-50 that did not agree with the termination effective date. We also noted that one of the sampled items stated, “termination due to payroll clean up per staffing January 2020 spreadsheet”.

Due to the fact that the payroll clean-up process only happens twice a year, employees could remain in the system for a period of time after they have abandoned their job. This may lead to the employee continuing to accrue and receive benefits that are paid by the agency, and the District incurring expenses that could have been avoided had the termination occurred early on.

In addition, because the employee is not promptly removed from the system once the individual is determined to have abandoned the job, the agency’s security systems are at risk for unauthorized access.

We discussed these noted conditions with DCPS’s Deputy Chief of Employee Services, who provided the following written explanation:

When our team identifies employees, whose schools have confirmed are not working, we start by checking paychecks to ensure that the employees have not been recently paid. The business rule that we've applied for cleanups is that an employee is eligible for termination if they haven't been paid in three months. There may be instances (like an expired temp hire, for example) where it's been less than three months, but we feel comfortable moving forward with the termination. But if we don't have much context on the employee, then 3 months is the baseline.

We also check email history to see if there are any extenuating circumstances that were previously flagged.

Based on these reviews, we pull together a list of employees who we believe should be terminated and send it to the following teams: Labor Management & Employee Relations, Benefits, Leave of Absence, Compensation. These teams will then check their own records to confirm if any of the employees should remain active for any reason. After these checks are completed, then we take the remaining employees and submit them to the Processing team for termination.

Typically, we are aggregating these lists based on audits connected with staff validations and/or Office of Chief Financial Officer-based budget reconciliation. These are mass clean-ups. The regular Not-To-Exceed (NTE) date expiration reviews, however, are done on a monthly basis and usually only require school level confirmation. The additional Employee Services teams are only looped in when there is a larger list of employees for whom we are unable to identify the reason for their active status.

Since Non-NTE employees who appear are added to the reports on a rolling basis, doing the audit monthly will likely capture them more quickly.

Recommendation: We recommend that the Chancellor of DCPS consider implementing a procedure that will track employees who have not reported to work/entered time in more than 30 days and report monthly to Human Resources for timely follow-up to ensure the individuals are deactivated from the system early enough to avoid the risks mentioned above.

Finding 2020-2. Lack of Approval on Notification of Personnel Action Forms

SF-50 forms should be approved and evidenced by a signature from the appropriate Human Resources administrator to ensure that only authorized changes are made to employees' files.

During our testing, we were unable to review approvals in the SF-50 for newly hired employees. We noted the District of Columbia Public Schools' current Peoplesoft configuration does not generate electronic signature approvals in the SF-50; nor are hard signatures obtained on the SF-50, to confirm and approve the change in personnel action. Therefore, payroll changes are completed without obtaining/maintaining the proper authorization in the employee file.

The lack of approval may result in unauthorized changes to employees' files. Additionally, the lack of application controls in PeopleSoft to prevent, detect, and correct unauthorized personnel changes may result in unauthorized or inaccurate changes being introduced into the Human Resources environment, and these changes may not be detected in a timely manner.

We discussed these noted conditions with DCPS's Deputy Chief of Employee Services, who provided the following written explanation:

We have taken the necessary steps to include an electronic signature of authorization to our SF-50 Form. A request was submitted to the Office of the Chief Technology Officer, (OCTO) to execute this change. We are optimistic this action will be completed within 30 days.

Recommendation: We recommend that the Chancellor of DCPS ensure that the configuration of PeopleSoft is corrected to align with other government agencies within the District to ensure that only authorized personnel changes are made in PeopleSoft to personnel profiles.

Implementing the above identified controls will help ensure only authorized and accurate personnel changes are made into the Human Resources environment at the District of Columbia Public Schools.

Department of General Services (DGS)

Finding 2020-3. Controls Over Compliance with the Quick Payment Act of 1984 Were Not Operating Effectively

We noted one instance related to the Department of General Services, where a vendor payment was made later than is required by the Quick Payment Act of 1984 (QPA), and the interest penalty due was not paid.

The vendor payment was made 53 days after receipt of the invoice, contrary to the required 30 days per QPA. Additionally, at the time of our audit, interest due as a result of this late payment was also not paid as required by QPA. The vendor had submitted a proper request for payment, and we were not made aware of any disagreements between the business and the agency. Additionally, given the amount of time that had lapsed before payment, all the requirements to automatically receive the required interest penalty payment were met.

Title 1 DCMR section 1700.3 (a) of the regulations that implement the QPA notes that agency heads have the responsibility “[t]o assure timely payments of proper invoices and the payment of interest for overdue payments;” The QPA regulations further provide guidance on the payment due date at section 1707.2 (c), which notes the payment due date is the “(30th) day after the receipt of a proper invoice by the designated payment officer.” District regulations also provide circumstances in which a business concern is entitled to automatically receive an interest penalty payment at sections 1709.1 (a-d).

There was a breakdown in the control environment and management did not have adequate oversight to ensure that all payments and interest penalty due were made within the guidelines set by QPA.

As a result of the conditions noted above, there is a risk that agencies will not be in compliance with the laws and regulations required by the Government of the District of Columbia (the District), as well as cause the District to be liable for interest penalty payments that could be avoided if the agencies followed the QPA.

We discussed these noted conditions with the Director of DGS, who provided the following written explanation:

OCFO reviewed the invoice history and determined that the delay that caused the QPA violation and interest penalty is not related to accounts payable operations. The OCFO internal controls over QPA compliance are designed adequately and operating effectively to ensure QPA compliance.

Accounts payable performs a routine review of QPA invoice log and follow up on outstanding invoices to ensure timely payments and compliance to QPA guidelines.

The invoice referenced above was submitted by the vendor on December 27, 2019. DGS Program staff completed all approvals (PASS receipt and Voucher) on January 22, 2020. Payment was approved/posted by AP on February 11, 2020 and the Payment released on February 18, 2020 via check. Based on the above, payment was issued in 53 days thus recorded and validated by the OCFO as a late payment of which \$166.27 was calculated and considered due to the vendor. OCFO communicated the violation to DGS and requested submission of a certification package for the payment of the interest. The interest payment of \$166.27 is pending reprogramming approval.

DGS acknowledged the delay and stated that it is due to various invoice discrepancies by the vendor. Going forward, the agency will be rejecting invalid invoices timely to prevent QPA violations.

Recommendation: We recommend that the Director of DGS ensure that oversight controls are strengthened so that controls over tracking compliance with QPA are working effectively. The controls should ensure that any potential overdue payments are timely addressed as well as any interest penalty payments due are appropriately paid.

Office of the Chief Financial Officer (OCFO)

Finding 2020-4. Controls Over Authenticator Management | Password-based Authentication Were Not Operating Effectively

OCTO's internal password policy does not match the Mainframe password configuration. The system configuration is set to automatically revoke inactive user IDs after 90 days. However, the entity's internal policy states that inactive users' IDs will be revoked after 30 days. We discussed this issue with the Director of Integrated

Platform Services and the Mainframe Services Information Technology Specialist, and the policy change was made to reflect the system password configuration that inactive IDs will be revoked after 90 days.

National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Rev. 5, AC-2 Account Management (f) states "Create, enable, modify, disable, and remove accounts in accordance with Mainframe Logon-id and Password Protection Policy. In addition, it is critical that the approved policy is implemented in the system configuration.

Management failed to ensure that their approved policy is implemented in the system configuration.

A discrepancy exists between management's approved policy and system configuration.

We discussed these noted conditions with OCFO's Chief Information Officer (CIO) who provided the following written explanation:

OCFO has reviewed the updated OCTO policy, which requires a password change every 30 days for active accounts and which invalidates a temporary password not used within 30 days. This policy exceeds the IRS Publication 1075 requirement that non-privileged accounts must be changed every 90 days and privileged accounts must be changed every 60 days and is acceptable to the OCFO. OCFO concurs with closing this NFR.

This situation was brought to OCFO management's attention and the policy was updated on October 15, 2020. However, this condition existed during the in-scope audit period and it is being reported as a finding. Management's subsequent actions in updating their policy closes this finding.

Finding 2020-5. Controls Over Reviews of Information Security Policies and Procedures Were Not Operating Effectively

We reviewed the information security policies and procedures that were in effect during the audit period. We determined that the information security policies and procedures were properly documented. However, we could not obtain supporting documented evidence that some of the policies were reviewed during FY 2020.

The following list includes information security policies for which we did not receive support documenting an annual review and the date of the last update:

1. OCIO Rules of Behavior V1 02/15/2018.
2. OCIO Collaborative Computing Policy and Procedures V1 02/08/2018.
3. Policies and Procedures Manual Volume I-A District-Wide Desk-Level Procedures 03/26/2018.

4. OCIO Physical Environment Policy and Procedures V1 05/24/2018.
5. DC Government MP Policy and Procedures 12/28/2018.
6. OCIO Access Control for Mobile Devices Policy and Procedures V1 02/08/2018.

These policies have not been updated since 2018.

OCFO and the Office of the Chief Information Officer (OCIO) have documented Policy and Procedures for the Audit and Accountability (AU) family of controls. The OCFO/OCIO used the Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies and the IRS Safeguards Program and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations to develop the security policy and procedures components which address the following:

At a minimum, the AU Policy and Procedures should be reviewed annually, and updated when new policy requirements are adopted, and/or new processes implemented.

There was a breakdown in the control environment that caused the listed policies and procedures not to be reviewed annually.

When information security policies and procedures are not reviewed and updated annually, outdated policies may exist. Outdated policies and procedures can increase the risk of security breaches.

We discussed these noted conditions with OCFO's CIO who provided the following written explanation:

Management agrees that a formal review process needs to be put into place to ensure that each policy is reviewed annually in conformity with its stated control policy and, where necessary, these six policies and procedures, should be updated to reflect any changes implemented based on the review. At a minimum, the annual review of policies and procedures should be documented in the revision history section where the review does not lead to a change in the published policy.

Recommendation: We recommend that the Chief Financial Officer of OCFO ensures that the agency develops, implements, and formalizes the process of annually reviewing information security policies and procedures to include maintaining the appropriate documentation of the reviews. Best practices for policy documentation include:

- a named person responsible for the policy or control procedures review;
- a statement within the policy to review the policy annually; and
- a revision history.

Finding 2020-6. Controls Over Least Privilege | Review of User Privileges Were Not Operating Effectively

We inspected the most recently completed VPN user access review, badge user access review, network user access review, operating system user access review, database user access review and application user access review, and we determined that some of the control self-assessments, including physical and logical access reviews, were not performed during the review period (FY 2020).

The OCFO/OCIO Information Security Group (ISG) has an automated process for reviewing accounts every 90 days. This process uses Active Directory (AD) Audit to analyze all AD accounts and report all inactive accounts. The report is sent to the OCFO/OCIO ISG. The CIO of OCFO/OCIO ISG reviews the report to validate the results. Accounts that are inactive are disabled manually after 90 days of inactivity as part of the report review.

NIST's SP 800-53, Rev. 5, AC-6(7) discusses Least Privilege | Review of User Privileges Control Activities. This section states, "The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid."

If the need cannot be revalidated, organizations should take appropriate corrective action.

There was a breakdown in the control environment regarding periodic access control reviews. Some stakeholders did not take adequate and timely actions to ensure that the reviews were completed.

The current situation where only some of the reviews are being performed increases the risk that users who no longer require access are not identified and that their access is not timely removed. It also increases the risk that users with unauthorized access may not be identified timely so that access can be appropriately removed or curtailed.

We discussed these noted conditions with OCFO's CIO who provided the following written explanation:

Management agrees that consistent implementation of the quarterly reviews is critical to ensuring access changes are made in a timely fashion and shall establish a schedule with each stakeholder to ensure the reviews are conducted.

Recommendation: We recommend that the Chief Financial Officer of OCFO ensures that the agency consistently follows the entity's internal access control review policy and ensures that all the relevant stakeholders complete the review.

Finding 2020-7. Controls Provide Reasonable Assurance That Employees Receive Proper Security Awareness Training

We tested a sample of twenty-five (25) new SOAR users and determined that four (4) out of the twenty-five (25) sampled did not complete the required security awareness training.

OCFO/OCTO Awareness and Training Policy and Procedures section 3.1, 3.2 and 3.3 discuss security awareness training on recognizing and reporting potential indicators of insider threat. It requires all information systems and applications owners to adhere to the following:

Provide basic security awareness training to information system users (including managers, senior executives, and contractors):

- As part of initial training for new users;
- When required by information system changes; and
- At least annually thereafter.

There was a breakdown in the control environment and management failed to enforce the existing policy and procedures. The OCFO Director of ERP Systems Group stated that these (4) new SOAR users were not setup as OCFO employees.

The lack of security awareness training for new SOAR users increases the risk of employees and contractors being susceptible to techniques used by third parties to gain unauthorized access to an organization's systems and information. Further, the lack of such training does not allow management to ensure that all system users understand their responsibilities to the District when using the District's systems.

We discussed these noted conditions with OCFO's CIO who provided the following written explanation:

All District employees are required to complete security awareness training each year. The OCIO is responsible for the OCFO security awareness training and conducts the annual training at the beginning of each calendar year. The four individuals were not set up in PeopleSoft properly and were not included in the OCFO training as a result. The OCIO will work with the SOAR Security Officer to improve the annual training process to confirm that all SOAR users are included in the OCFO training. The OCIO will also work with the OCFO HR department to establish a process to ensure all new OCFO hires are required to complete security awareness training.

Recommendation: We recommend that the Chief Financial Officer of OCFO ensures that the agency implements appropriate control measures to ensure that new hires receive security awareness training upon hire and on an annual basis thereafter. Documentation should be maintained demonstrating that such security awareness training was provided and completed by each employee.

Department of Employment Services (DOES)***Finding 2020-8. Controls Over Reviews of Information Security Policies and Procedures Were Not Operating Effectively***

We reviewed the information security policies and procedures for DOES and determined that organizational and information security policies and procedures were documented. However, most of the policies reviewed have not been reviewed/updated for more than two years.

The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

According to all policies and procedures reviewed, revision is supposed to be carried out annually. Also, NIST SP 800-53, Rev. 5 Control Identifier family AC-1, AU-1, MA-1 discusses Periodic Review of Control Activities. This section states, "Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. If there is a significant change in an entity's process, management reviews this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, or information technology.

There was a breakdown in the control environment and management. The entity has not reviewed the following listed information security policies for accuracy and applicability on an annual basis:

1. Access Control Policy (DOES) - March 2017
2. Change Control Policy (DOES) - March 2017
3. Configuration Management (DOES) - March 2017
4. Data Integrity Policy (DOES) - March 2017
5. Remote Access Policy (DOES) - March 2017
6. Security Incident Reporting and Response (DOES) - September 2014
7. System & Service Acquisition (DOES) - March 2017
8. System Maintenance Policy (DOES) - September 2014
9. Information Technology Acceptable Use (DOES) - March 2013
10. Confidential Data & Systems Management Policy (DOES) - March 2019

Due to the information security policies listed above not being reviewed annually, there is an increased risk that the policies are not accurate, valid, or applicable.

We discussed these noted conditions with DOES's CIO, who provided the following written explanation:

DOES Office of Information Technology (OIT) Management concurs with the Notification of Findings and Recommendation. While the policies listed are overdue for the bi-annual update, each DOES OIT Security Policy is reviewed each year as required. The "most recent cycle's" sign-offs, however, have been delayed due to the agency going through a management transition process (just fully onboarded in January of 2020), as well as the pandemic impact on agency operations.

The following policies are currently undergoing review to reflect the security posture of the agency. These will be finalized, signed, and distributed to all DOES employees and contractors before January 1, 2021.

- OIT_DOES_SEC_001 Access Control Policy
- OIT_DOES_SEC_002 Change Control Policy
- OIT_DOES_SEC_014 Remote Access Policy
- OIT_DOES_SEC_006 Incident Reporting and Response Plan
- OIT_DOES_SEC_007 System and Services Acquisition Policy
- OIT_DOES_SEC_011 Systems Maintenance Policy
- OIT_DOES_SEC_003 Agency-Wide Computer and Acceptable Use Policy
- OIT_DOES_SEC_005 Confidential Data and Systems Management Security Policy

The owner of each of these is the Chief Information Officer; they are to be reviewed annually by the OIT Leadership Team and Chief Information Security to all DOES employees and contractors as required.

The 8 policies listed in the written explanation above represent 8 of the 10 policies listed in the noted conditions above.

Recommendation: We recommend that the Director of DOES ensures that department develops, implements, and formalizes policies and procedures for the control activity. Best practices for policy documentation include:

- a named person responsible for the policy;
- a statement to review the policy annually; and
- a revision history.

Finding 2020-9. Controls Over Terminated User Access Are Ineffective

In the process of testing the sample of terminated users, an individual on the District Online Compensation System's (DOCS) terminated user list was found to be listed as active on the DOCS' User Access list. The individual was terminated on May 8, 2020, and remained active in the time system until November 2020. A subsequent investigation found that other individuals terminated in 2016 and 2018 also remained on the active user list.

An individual on the District of Columbia Unemployment Tax Accounting System's (DUTAS) terminated list was terminated on February 12, 2020, but their access was not terminated from DUTAS until June 23, 2020.

NIST's SP800-53 Revision 5, AC-2(3) Disable accounts within [Assignment: organization-defined time period] when the accounts:

- a. Have expired;
- b. Are no longer associated with a user or individual;
- c. Are in violation of organizational policy; or
- d. Have been inactive for [Assignment: Mainframe Logon id and Password Protection Policy states inactive accounts will be revoked after 90 days].

Office of the Chief Technology Officer:

Integrated Platform Services Division Mainframe Logon id and Password Protection Policy, version 2.1, Last Revised/Reviewed Date: October 15, 2020 states:

“S.12. Inactivity Logon-ids will be revoked automatically when they are inactive for more than 90 days.”

Procedures around the termination of users are not being followed.

As a result of the conditions noted above, users that should not have access to the system are being allowed to remain active. This increases the risk that unauthorized users may access and make changes to the system.

We discussed these noted conditions with DOES's HR Officer, who provided the following written explanation:

DOES Human Resources Management accept the Notification of Findings and Recommendation. DOES-HR has drafted new off-boarding policies that require program staff to timely notify HR of resigning and retiring employees, upon receipt of notice, to facilitate the timely disabling of access to agency systems. Agency staff will be trained and ask to acknowledge the policy upon approval of the draft policy by the agency Director.

Agency staff will be notified, in writing, of their responsibilities in the new off-boarding process within 45 days of Director's approval of policy. HR staff will also be trained on the new off-boarding process and notification requirements to ensure timely disabling of access to systems agency wide. To facilitate proper off-boarding, HR staff is responsible for notifying OIT of the employee's separation on the effective date.

Recommendation: We recommend that the Director of DOES ensures that the department implements control measures to ensure the timely revocation of access for terminated or separated personnel.

Finding 2020-10. Controls Over Security Awareness Training and Policy Acknowledgment Procedures Were Not Operating Effectively

We tested samples of new hires and current active user populations and determined that a significant number of users in each sample did not complete the required security awareness training. Three (3) of the twenty (20) new hires and seven (7) of sixty (60) current users of DOCS were determined not to have completed the required training. One (1) of five (5) new hires and nine (9) of twenty (20) current users of DUTAS were determined not to have completed the required training. Three (3) of the twenty (20) new hires with access to DOCS did not sign policy acknowledgement documents.

Section 4.2 of the Government of the District of Columbia Awareness and Training (AT) Policies and Procedures states:

OCFO/OCIO requires all information systems and applications owners to adhere to the following:

- a. Provide basic security awareness training to information system users (including managers, senior executives, and contractors):
 1. As part of initial training for new users;
 2. When required by information system changes; and
 3. At least annually thereafter.

All OCFO / OCIO employees, contractors, and interns are required to complete security awareness training prior to gaining access to OCFONet, information systems, and applications, including access to Federal Tax Information (FTI), when their roles and responsibilities change in relation to assigned information systems and applications, and annually thereafter. The security awareness training is administered via the KnowBe4 online training provider.

- a. Include security awareness training on recognizing and reporting potential indicators of insider threat. (CE2)

Insider threats and recognizing and reporting potential indicators of insider threat training modules are included as part of the KnowBe4 and UNAX security awareness training.

Management failed to enforce the existing policies and procedures.

The lack of periodic security awareness training increases the risk that employees and contractors will be susceptible to techniques used by hackers and other threat sources to gain unauthorized access to systems and information. Further, the lack of such training does not allow management to ensure that all system users understand their responsibilities to the District when using the District's systems.

We discussed these noted conditions with DOES's CIO, who provided the following written explanation:

DOES OIT Management concurs with the Notification of Finding and Recommendation. Due to the agency's need to rapidly onboard users to support the agency's COVID response, we began processing multiple users simultaneously. Which inadvertently bypassed the system's security training check that looked to see if the user had taken security training with-in the last year.

To remedy the issue and to ensure that this doesn't reoccur, the request system is being updated with a popup reminder to the requestor to process only one user per ticket; the estimated delivery date will be January 15, 2021. We will modify the Access Control Policy to update the frequency of internal audits. Lastly, we will train everyone in the approval process on how to process user account requests properly.

As of October 27, 2020, all DOES users have been enrolled in Security Training, due by December 31, 2020. Those users who fail to complete their training by December 31, 2020, will have their access revoked.

The owner of this process is the Chief Information Officer with the support of the OIT Leadership Team and the Chief Information Security.

Recommendation: We recommend that the Director of DOES ensure that the department implements detective and corrective controls to ensure that all employees and system users complete the required training and sign the required acknowledgment forms.

Office of Contracting and Procurement (OCP)

Finding 2020-11. Controls Over Emergency Procurement Were Not Operating Effectively

The District of Columbia's Mayor's Order 2020-045 declared a Public Emergency due to the impact of the COVID-19 coronavirus and the resulting pandemic. The Mayor's Order 2020-046 declared a public health emergency due to the pandemic. The District has incurred approximately \$195 million of expenditures to combat the spread of COVID-19, much of which were acquired through the use of emergency procurement

procedures. From this population, we selected for testing 23 transactions that were paid through standard disbursement procedures, 68 transactions that were paid through direct voucher procedures, and 10 transactions which were paid by using a District approved purchasing card (P-card).

For the COVID-19 emergency procurement transactions that were paid through standard disbursement procedures, we were unable to obtain the following:

- For two samples, MJ did not receive definitized contracts. These two samples were regular procurement transactions, in excess of \$100,000. The Office of Contracting & Procurement (OCP) confirmed that these procurements should have had contracts issued.

For those COVID-19 emergency procurement transactions that were paid through direct voucher procedures, we were unable to obtain the following:

- For 18 samples, MJ was not provided with documentation of receipt and acceptance of goods and/or services. Contracts, vendor invoices, voucher approvals and general ledger evidence of the recorded payments were provided, but documentation of the District receiving the quantities of items procured was not provided.
- For 18 samples, MJ received Bills of Lading (BOL) which could not be used to verify receipt and acceptance of goods and/or services procured. The District bought large quantities of personal protective equipment (PPE), and these items were typically delivered by third party shipping companies. The deliveries of PPE were received by warehouse and logistics personnel. For these samples, no indication of the number of units delivered was provided, whether typed or handwritten. Our testing yielded other samples that were successfully tied out, either by number of units or numbers of cases and quantities of units per case, but these transactions were not.
- For one sample, MJ did not receive a Voucher Approval, which is required to release a payment to the vendor. The payment was made to the vendor, and the payment agreed with the contract, invoice and receipt documentation. However, the approval to pay the voucher was not provided.
- For two samples, the required notice to Council within 7 days after the execution of a contract procured using emergency procurement methods was not made.

DC Official Code Section 7-2304(b), as enacted by the COVID-19 Response Emergency Act of 2020 indicates that *“a summary of each emergency procurement entered into during a period for which a public health emergency is declared shall be provided to the Council no later than 7 days after the contract is awarded. Such summary shall include a description of the goods or services procured; the source selection method; the award amount; and the name of the awardee.”*

Prudent business practices discourage the advance payments or prepayments for goods and services whenever possible. However, when instances warrant the prepayment of goods and services, a process to document the justification for prepayment should exist and be followed. Further, documentation of the receipt of those goods or services, even if procured using an emergency procurement method, should be obtained and retained.

Failure to maintain appropriate supporting documentation for transactions procured using approved emergency procurement methods increases the risk that the cost of items procured under a valid emergency procurement procedure will be disallowed for reimbursement. Further, failure to maintain documentation justifying the need for prepayment, including documenting when it is anticipated that those goods or services will be received, increases the risk that those goods or services which have been prepaid may not be received. Finally, failure to make the required 7-day timely notice of emergency procurements made during the pandemic does not allow Council to exercise its oversight responsibilities as required by law.

We discussed these noted conditions with the Chief Operating Officer of OCP, who provided the following written explanation:

Condition #1: For two samples, MJ did not receive definitized contracts. These two samples were regular procurement transactions, in excess of \$100,000. The Office of Contracting & Procurement (OCP) confirmed that these procurements should have had contracts issued.

District Comment: OCP clarified the letter contract terms to CAFR Audit team. Still, they erroneously concluded that the requirement to definitize a contract is based solely on the contract value.

OCP did not confirm that “procurements should have had contracts issued.” OCP stated that in instances where the contractual supplies and services were received by the District within the letter contract period, the letter contracts may have been allowed to expire without definitizing the contracts. Therefore, it is the completion of the contract terms within the letter contract period that determines the requirement for a definitized contract, not the contract value.

Condition #4: For one sample, MJ did not receive a Voucher Approval which is required to release a payment to the vendor. The payment was made to the vendor, and the payment agreed with the contract, invoice and receipt documentation. However, the approval to pay the voucher was not provided.

District Comment: An OFOS approval confirmation email couldn't be retrieved for one of the payments. However, GOC request and approval was provided for this item. OFOS reported that Miscellaneous DV payment authorization will be documented as part of the final DV package in FY2021. The implementation of this change will also be incorporated as part of policy and procedure update.

Effect: Failure to maintain appropriate supporting documentation for transactions procured using approved emergency procurement methods increases the risk that the cost of items procured under a valid emergency procurement procedure will be disallowed for reimbursement.

District Comment: With the understanding that past federal reimbursement performance is not an indication or guide for current or future federal reimbursement performance, we note that there have been no instances in at least the preceding five fiscal years where costs incurred by OCP under a declared emergency have been disallowed for federal reimbursement for any reason, including lack of adequate supporting documentation.

As is noted in the NFR, albeit without context, is that to date the District has incurred in excess of \$195M of expenditures while managing its response to the COVID-19 pandemic. What is not mentioned, is that the District has also received federal reimbursement of more than \$195M in COVID-19 expenditures based on the same supporting documentation that was submitted to the CAFR Audit team for their internal control testing procedures.

Note also that FEMA's public assistance reimbursement grants management portal comprises a multistep review and approval process. The steps are outlined below.

1. Recipients attend virtual applicant briefing
2. Log on and create account at Public Assistance (PA) Grants Portal
3. Submit a Request for Public Assistance (RPA)
4. Submit a COVID-19 Streamlined Project Application
5. FEMA and Recipient review documents
6. Applicant Signs Project
7. Receive funding through Recipient

FEMA reviews information submitted online including work activities, costs, and supporting documentation and contacts the Recipient if there are any questions.

While we acknowledge cost disallowance is a valid risk overall, we note that the District and OCP in particular, has demonstrated compliance with FEMA policy and its own emergency procurement documentation policies and procedures, as evidenced by FEMA's acceptance and reimbursement of more than \$195M in allowable COVID-19 expenditures.

McConnell and Jones LLP response – We have read and evaluated the District’s response. The District has chosen not to furnish a response to the second, third, and fifth bulleted items referred to above on page 14. We have considered what the District has chosen to respond to, and our finding remains as presented.

Recommendation: We recommend the Chief Operating Officer of OCP ensure that all applicable documentation supporting the procurement of and payment for goods and services procured using emergency procurement processes is maintained and that appropriate, timely notification be made to Council of such emergency procurements as required by law.

II. STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

The following chart outlines the status of prior year management recommendations and business recommendations that had not been implemented as of September 30, 2020.

MANAGEMENT RECOMMENDATIONS – FY19		
RECOMMENDATIONS		STATUS
HOME PURCHASE ASSISTANCE PROGRAM		
1	Maintain Loan Receivable File Support	Complete process of improving controls around loan files support.

MANAGEMENT RECOMMENDATIONS – FY18		
RECOMMENDATIONS		STATUS
GENERAL GOVERNMENT		
3	Implement a Risk Management Framework to Comply with National Institute of Standards and Technology (NIST) Publication 800-37	Management has hired a Government, Risk and Compliance officer who will complete the appropriate policy review and changes as well as develop the risk management strategy.
7	Improve the Controls Over the Out-Lease Monthly Cash Receipts	Management should implement an automated tracking system for out-lease agreements cash receipts.

MANAGEMENT RECOMMENDATIONS – FY17		
RECOMMENDATIONS		STATUS
GENERAL GOVERNMENT		
2	Maintain Files Supporting Medicaid Eligibility	Management to complete organization of the supporting files to support eligibility.
OFFICE OF LOTTERY AND CHARITABLE GAMES		
2	Develop Vulnerability Scan Procedures for Timely Remediation of Critical Risks	Subsequent the close of the fiscal year steps were completed by the organization to resolve the prior year recommendation.