USDA

United States Department of Agriculture

Office of the Chief Financial Officer

National Finance Center

P.O. Box 60000
New Orleans
Louisiana 70160

Date:
11/19/20

In reply refer to:

Subject: Year-End A-123 Statement of Assurance

To: Customers and Stakeholders

As a Federal service provider for Agencies of the Department Agriculture (USDA), as well as many non-USDA Agencies, the National Finance Center (NFC) is subject to numerous legislative and regulatory requirements that are satisfied through internal control testing. Annual reviews of NFC's internal controls over financial reporting are performed to satisfy Office of Management and Budget (OMB) Bulletin 19-03, *Audit Requirements for Federal Financial Statements*, and OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. As suggested by both OMB Bulletin 19-03 and A-123 guidance, NFC meets these requirements by providing our customers a System and Organization Controls 1 (SOC 1) type 2 report conducted in accordance with Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

KPMG LLP (KPMG) conducted a SOC 1 type 2 examination in accordance with SSAE 18 of NFC's payroll/personnel system for the period of October 1 through June 30, 2020. KPMG issued the report on October 30, 2020 (this was the date on KPMG's opinion letter). The Office of Inspector General (OIG) added an OIG transmittal letter dated November 4, 2020, and published the report.

The report stated the adverse opinion was rendered based on the following two control design deficiencies:

- The description states that controls are in place to provide reasonable assurance that access to programs, data, and computer resources relevant to user entities' internal control over financial reporting is restricted to authorized users, processes, and devices. However, NFC did not suitably design controls to authorize, restrict, and monitor access to super user system identifications. As a result, controls were not suitably designed and operating effectively to achieve the control objective: "Controls provide reasonable assurance that access to programs, data, and computer resources relevant to user entities' internal control over financial reporting is restricted to authorized users, processes, and devices."

- The description also states that controls are in place to provide reasonable assurance that changes to application programs are authorized, tested, documented, approved, and implemented to support the complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities' internal control over financial reporting. However, NFC did not suitably design controls to prevent or detect changes

> to mainframe application production and baseline libraries made outside of the established change management procedures. As a result, controls were not suitably designed and operating effectively to achieve the control objective: "Controls provide reasonable assurance that changes to application programs are authorized, tested, documented, approved, and implemented to support the complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities' internal control over financial reporting."

Regarding the first design deficiency, as part of their testing, KPMG reviewed the form approving the use of the super user account for the seven instances where it was used during the scope of the examination. For two of these seven instances, only one of the three required approvals was obtained before the account was used, and in a third instance, only one of the three required approvals was obtained before the form was requested by KPMG. KPMG further elaborated in the Notice of Findings and Recommendations that management included some details of the control activities in the system description; however, formal policy, procedures, and processes did not exist that defined the events or business needs that would require the use of this powerful account, when the form used to approve the use of the account should be completed, or for reviewing the activity performed with the super user account to ensure that it was authorized and appropriate.

NFC and the Office of the Chief Information Officer (OCIO) provided additional evidence documenting that the super user account was only used when needed to grant access that had been authorized in accordance with formally documented procedures included in the system description (i.e., NFC-1106, Security Access Request, process). NFC does have other controls documented in the system description that would mitigate the impact on the control objective if the super user account had been used inappropriately. These mitigating controls include: monitoring critical mainframe activities, quarterly role-based access reviews, and annual reviews of access to critical mainframe applications. In addition, as part of their testing of the formal NFC-1106 process, KPMG tested for unauthorized access to critical applications and mainframe resources and did not report any exceptions.

Regarding the second design deficiency, KPMG reported that the weekly review of the report of updates made to the mainframe outside of the change management software (ChangeMan ZMF) was not suitably designed as one of the individuals performing the review also performs updates to the mainframe environment, and the secondary review to compensate for the incompatible duties of the first reviewer did not occur during the scope period. The system description states that NFC uses change management software to maintain application baselines throughout the system development lifecycle but did not specifically state that the mainframe change management software prevents changes made outside of the configuration management system from being implemented into the production environment. Because this was a SOC 1 attestation examination, the audit was limited to testing the control activities as

described in the system description. If control activities exist at the service organization but are not specifically described in the system description, per the standard those control activities would not be considered.

Upon further reflection and analysis, we determined that, in some cases, the control activities included in the NFC SOC 1 system description were overly prescriptive and did not allow flexibility for adjustments when circumstances require flexibility. To rectify some of the issues encountered during the fiscal year 2020 examination, we will modify the control activity descriptions to bring them in line with actual practices. In addition, we will review the control activity descriptions, as they are currently written, to identify potential control gaps that may exist and revise the control activity descriptions where needed and/or implement additional controls to address any gaps identified. Furthermore, while we understand the severity of the opinion, we firmly believe the control deficiencies reported would not result in material misstatements to payroll that would impact agency financial statements.

NFC and OCIO are committed to making the needed corrective actions to address the deficiencies as soon as possible. We are in the process of implementing corrective actions now and plan to have all corrective actions in place no later than January 31, 2021.

/S/
CALVIN W. TURNER JR.
Director