RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

February 01, 2024

Tina Donbeck

Chief Information Officer
United States International Development Finance Corporation
1100 New York Ave, NW
Washington, D.C. 20527

Anthony Zakel
Inspector General

Ref: Development Finance Corporation's *Federal Information Security Modernization Act of 2014 Audit*

Dear Ms. Donbeck and Mr. Zakel,

RMA Associates, LLC (RMA) was contracted by the United States International Development Finance Corporation Office of Inspector General (DFC OIG) to conduct a performance audit of DFC's information security program in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

RMA is responsible for conducting our performance audit to determine whether DFC implemented an effective information security program[1].

Performance Audit Objectives and Scope

On December 18, 2014, the President signed the *Federal Information Security Modernization Act of 2014* (FISMA), which amended the *Federal Information Security Management Act of 2002* (FISMA 2002) and provided several modifications that modernize Federal security practices to address evolving security concerns.

FISMA requires Federal agencies to conduct an annual independent assessment of their information security program and practices to determine the effectiveness of such programs and practices and report the assessments' results to the Office of Management and Budget (OMB).

The Fiscal Year (FY) 2023-2024 *IG FISMA Reporting Metrics* will represent a continuation of work begun in FY 2016 when the IG's FISMA reporting metrics were aligned with the five (5) function areas in the National Institute of Standards and Technology (NIST) *Framework for*

[1] For this audit, an effective information security program is defined as having an overall mature program based on the current year inspector general FISMA reporting metrics.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identity, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise. It provides the IGs with guidance for assessing the maturity of controls to address those risks. RMA will use the FY 2023-2024 *IG FISMA Reporting Metrics*, developed as a collaborative effort by OMB, Department of Homeland Security (DHS), and the Council of Inspectors General on Integrity and Efficiency (CIGIE) in consultation with the Federal Chief Information Officer Council.

As required by task order number 140D0421F0244, RMA is responsible for conducting our performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Under those standards, our audit engagement meets the definition of a performance audit. It requires that we plan and conduct the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our performance audit objectives.

The performance audit is designed to determine whether DFC implemented an effective information security program that supports the FISMA. Our performance audit will be conducted for FY 2024. It will test the group of core metrics, which represents a combination of administration priorities and other highly valuable controls selected by OMB that must be evaluated annually. Additionally, we will test the supplemental metrics of Group 2, which represent a combination of metrics that must be evaluated on a two-year cycle based on a calendar agreed to by CIGIE, the Chief Information Security Officer (CISO) Council, OMB, and Cybersecurity and Infrastructure Security Agency (CISA). The remainder of the standards and controls will be evaluated in FY 2025.

To conduct our performance audit of DFC's information security program and practices, we will consider NIST Special Publication (SP) 800-53A*, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans;* SP NIST SP 800-53*, Security and Privacy Controls for Federal Information Systems and Organizations;* and the FISMA guidance from CIGIE, OMB, and DHS.

We will review the legal and regulatory requirements stipulated in FISMA and conduct interviews with DFC officials and contractors to determine if DFC implemented an effective information security program.

Additionally, we will review documentation supporting the information security program. These documents include but will not be limited to DFC's (1) risk management policy, (2) configuration management procedures, (3) identity and access control measures, (4) security awareness training, and (5) continuous monitoring controls. We will compare documentation against the requirements stipulated in NIST SPs. Also, we will perform tests of information system controls to determine the effectiveness of those controls.

Our testing procedures are developed from NIST SP 800-53A. We will determine the overall maturity level of each of the nine domains under the FY 2024 *IG FISMA Reporting Metrics* guidance. However, until the FY 2024 *IG FISMA Reporting Metrics* are issued, we will test using

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

the guidelines, including the FY 2023-2024 *IG FISMA Reporting Metrics* published in February 2023, the President's Executive Order 14028, Improving the Nation's Cybersecurity and OMB M-24-04: *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements.*

If this engagement does not satisfy the requirements of all performance audit report users, laws, and regulations, we will notify management and those charged with governance as soon as this comes to our attention. We will then submit another engagement letter for management's approval that complies with the applicable requirements and will seek approval for the engagement.

If we discover any potential observations or findings, we will disclose them to management and those charged with governance in advance. Management will be allowed to provide a response expressing agreement or disagreement with each finding.

If, for any reason, we are unable to complete the performance, we may decline to issue a report as a result of this engagement. We will notify management and those charged with governance if such a situation arises.

Additionally, RMA will issue a draft and final performance audit report that addresses the identified risks and makes recommendations to assist the agency with alleviating challenges.

Management's Responsibilities

Management is responsible for providing RMA with all requested records and related information to conduct the performance audit by the due date identified in the Provided by Client (PBC) list. It is also responsible for the accuracy and completeness of that information. In extenuating circumstances, RMA may accept PBCs, but no PBCs will be considered after Friday, June 14, 2024. If management is unable to provide the requested information, RMA will document such in its reporting if it may present a material effect on the performance audit results. Additionally, management is expected to make a reasonable effort to be available for performance audit procedures and enforce that standard among staff members to enable an efficient performance audit process, including documentation requests, interviews, meetings, walkthroughs, and other requirements.

Management is responsible for the design, implementation, and maintenance of programs and controls to prevent and detect fraud and for informing us about all known or suspected fraud or illegal acts affecting the government involving (1) management, (2) employees who have significant roles in internal control, and (3) others where the fraud or illegal acts could have a material effect on reported data. Management's responsibilities include informing us of any fraud or suspected fraud allegations affecting the government received in communications from employees, former employees, regulators, or others.

In addition, management is responsible for identifying and ensuring compliance with applicable laws, regulations, contracts, and agreements. Furthermore, it is management's responsibility to follow up and take corrective action on reported findings and prepare a summary schedule of prior

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

findings and a corrective action plan. The summary schedule of prior findings should be available for our review upon request.

Management is responsible for establishing and maintaining a process for tracking the status of findings and recommendations. Management is also responsible for identifying previous audits or other engagements or studies related to the objectives discussed in the Audit Objectives and Scope section of this letter. This responsibility includes relaying corrective actions to address significant findings and recommendations from those audits or other engagements or studies. Management is also responsible for providing views on findings, conclusions, recommendations, and planned corrective actions.

Auditor's Responsibilities – General Audit Procedures

The performance audit will include examining the evidence on a test basis and measuring against criteria stipulated in Federal regulation, agency policy and procedures, and other applicable guidance. We will plan and conduct the performance audit to obtain reasonable rather than absolute assurance about whether procedures are designed appropriately and implemented effectively.

Our responsibility as auditors is limited to the period covered by our performance audit and does not extend to any later periods for which we are not engaged as auditors. There is a risk that control deficiencies or noncompliance may exist and not be detected by us since not all data will be tested. In addition, the performance audit is not designed to detect control deficiencies or violations of laws or government regulations that do not directly or materially affect our performance audit objective. Nonetheless, if we become aware of such errors, fraud, or illegal acts during our performance audit, we will bring them to your attention and notify the IG in writing and the appropriate enforcement agency.

Auditor's Responsibilities – Internal Controls Audit Procedures

The performance audit will include obtaining an understanding of the entity and its environment, including internal controls, sufficient to assess the risks of procedures. Tests of controls may be performed to test the effectiveness of certain controls that we consider relevant to preventing and detecting errors and fraud that are material to reported data and preventing and detecting control deficiencies resulting from illegal acts and other noncompliance matters that have a direct and material effect on reported data. The test will also measure the quality of the design of internal controls and their related operational effectiveness.

Throughout the performance audit, we will communicate to management and those charged with governance of internal control-related matters.

Auditor's Responsibilities – Compliance Audit Procedures

RMA will access the overall maturity level of each of the nine domains under the FY 2024 IG FISMA Reporting Metrics guidance. However, until the FY 2024 IG FISMA Reporting Metrics are issued, we will test using the guidelines, including the FY 2023-2024 *IG FISMA Reporting*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Metrics published in February 2023, the President's Executive Order 14028, Improving the Nation's Cybersecurity and OMB M-24-04: *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements.*

Auditor's Responsibilities – Audit Administration

Upon completion of the engagement, we will send a copy of the report to DFC OIG, and OIG will send a copy of RMA's report to DFC. The report shall describe the scope of testing, testing methodology, the results of the tests, and, if applicable, any findings and management's corrective action plans (CAP).

Our performance audit will include a review of any relevant prior-year suggestions and recommendations. It will indicate the extent to which the summary schedule of prior year findings is fairly stated. As to any current-year recommendations and suggestions, we will allow management to respond to such matters and include your response(s) in management's CAP.

After the issuance of the report, should it be necessary to alter or reissue the report and/or any management letter, OIG will transmit the report and/or management letter in the same manner as the original report and management letter.

Performance Audit Coordination and Other Matters

We believe this letter accurately summarizes the significant terms of our engagement. If management and those charged with governance agree with the terms and arrangements outlined in this letter, we request your signature below and return the agreement to us.

This assignment will be conducted under my direction, Reza Mahbod, Partner, and I can be reached at (202) 285-5868 or by email at ***R.Mahbod@RMAFed.com*** and George Fallon, Director, who can be reached at (410) 336-8454 or by email at ***G.Fallon@RMAFed.com***. Should this letter not represent your understanding of the nature of this engagement, or you have any questions or need further information, please contact me.

We look forward to a successful engagement.

Very respectfully,

Reza Mahbod

Reza Mahbod, Partner

(202) 285-5868

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Management's Acknowledgment of the Engagement Terms

On behalf of DFC, its management, and those charged with governance, I acknowledge and agree to the terms and arrangements described above for the FISMA performance audit of DFC's information systems.

This letter correctly sets forth the understanding of OIG.

TINA DONBECK Digitally signed by TINA DONBECK Date: 2024.02.01 07:33:33 -05'00'

Signature **Date**

Ms. Tina Donbeck
Vice President and Chief Information Officer

Anthony Zakel January 23, 2024

Signature **Date**

Mr. Anthony Zakel
Inspector General

cc:

Darrell Benjamin
Contracting Officer Representative
Deputy Inspector General

George Fallon
Director, RMA Associates, LLC