U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: November 12, 2020

Subject: INFORMATION: Audit Announcement | Review of Security Controls for FTA's Financial Management Systems That Support CARES Act Funding | Project No. 21T3001T000
Federal Transit Administration

From: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

To: Chief Information Officer, Department of Transportation
Associate Administrator for Budget and Policy, Federal Transit Administration

The national transportation system supports the American economy by facilitating jobs, businesses, and our way of life. However, the transportation industry has been seriously impacted by the current coronavirus disease pandemic. In March 2020, the President signed the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[1] This law provides emergency assistance and health care responses for individuals, families, and businesses, and emergency appropriations to support executive branch agency operations during the pandemic.

Under the act, the Department of Transportation (DOT) has received over $36 billion in funding to provide emergency assistance to the transportation industry. Of this $36 billion, the Federal Transit Administration (FTA) has received $25 billion.[2] The act authorizes FTA to use these funds to provide grants for transit infrastructure to prevent, prepare for, and respond to the pandemic. FTA uses several financial management systems to approve, monitor, and distribute CARES Act funds.

Since March 2020, the number of attacks on Federal Government information systems has increased through a variety of techniques, including social engineering and spear phishing. These attacks can hinder Federal agency operations and threaten the operations of FTA's financial management

[1] Pub. L. No. 116-136.
[2] FTA is allocating $25 billion to recipients of urbanized area and rural area formula funds, with $22.7 billion to large and small urban areas and $2.2 billion to rural areas.

information systems by affecting system and information confidentiality,[3] availability,[4] and integrity.[5] For example, an attack can result in a system outage through denial of service, or expose personally identifiable information and result in a data breach.

In addition, the Agency is required to select security controls that are designed to reduce systems' vulnerability, minimize risk, and meet minimum security requirements defined in Federal Information Processing Standards Publication 200.[6] Accordingly, we are initiating this audit to assess the effectiveness of FTA's financial management systems' security controls designed to protect the confidentiality, integrity and availability of the systems and their information.

We plan to begin work immediately, and will conduct the audit remotely at DOT Headquarters and contractor sites as necessary. We will contact your audit liaison to schedule an entrance conference. If you have any questions, please call me at (202) 366-1518, or Nathan Custer, Program Director, at (202) 366-5540.

cc: DOT Audit Liaison, M-1
FTA Audit Liaison,

[3] Confidentiality refers to the security service that aims to ensure that information is only provided to the intended individual or group.
[4] Availability refers to the security service that aims to ensure that an information system may be accessed upon the request of a user.
[5] Integrity refers to the security service that aims to ensure that data containing information remains unaltered during transit.
[6] Federal Information Processing Standards Publication 200 details how Federal agencies must meet the minimum security requirements through the use of the security controls in accordance with National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, as amended.