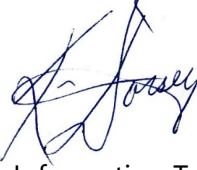# Memorandum

Date:	November 1, 2021
Subject:	INFORMATION: Audit Announcement | Review of DOT's Cloud Services Program | Project No. 21T3005T000 Department of Transportation
From:	Kevin Dorsey Assistant Inspector General for Information Technology Audits
To:	Chief Information Officer

In 2011, the Office of Management and Budget issued its Federal Cloud Computing Strategy[1] which required agencies to use cloud infrastructure, as they planned new missions, supported applications, or consolidated existing applications. In 2019,[2] the Federal Cloud Computing Strategy was updated, tasking Federal agencies—including the Department of Transportation (DOT)—to accelerate migration to cloud-based computing solutions and modernize information technology (IT) infrastructure. The strategy focused on enhancing security and high-quality IT service to the American people. In May 2021, the President issued an Executive order[3] detailing his administration's goal to modernize Federal Government cybersecurity. Specifically, to keep pace with today's dynamic and increasingly sophisticated environment, the Federal government should accelerate the movement to secure cloud services, adopt security best practices, and develop migration plans for Zero Trust Architecture.[4]

With the increase in Federal agencies using cloud services, we are self-initiating this audit to assess DOT's oversight of its cloud services and the overall effectiveness of its cloud systems' privacy and security controls. Accordingly, our audit objectives are to assess the effectiveness of the Department's (1) cloud

---

[1] The Federal Cloud Computing Strategy is a long-term, high-level strategy to increase cloud computing service adoption at Federal agencies.

[2] Office of Management and Budget, *Federal Cloud Computing Strategy*, June 24, 2019.

[3] Executive Order 14028, *Improving the Nation's Cybersecurity*, May 2021.

[4] Zero Trust Architecture is a type of cybersecurity plan built on the concept that we cannot assume devices and networks can be trusted. It also encompasses component relationships, workflow planning, and access policies.

systems' security and privacy controls and (2) strategy to secure cloud services in order to implement Zero Trust Architecture.

We plan to begin the audit immediately and will contact your audit liaison to schedule an entrance conference. We will primarily conduct our work at DOT Headquarters in Washington, DC. but may make site visits to contractor facilities as necessary.   If you have any questions, please contact me at 202-366-1518, or Nathan Custer, Program Director, at 202-366-5540.

cc: DOT Audit Liaison, M-1