General Services Administration
Rideshare/Ride-hail Privacy and Security Overview

Who:
The General Services Administration (GSA) has partnered with Uber (Uber for Business (U4B)) and Lyft, Inc. (Lyft Business System) to provide GSA federal agency customers' transportation solution and services to federal employees and contractors through a platform that leverages the existing Rideshare/Ride-hail vendor's web-based dashboard, infrastructure, and driving community.

What:
The rideshare/ride-hail vendor's online dashboard provides organizations a more efficient way to manage their business travel and improve their employees' travel experience. Each vendor's web-based portal provides agencies with access to employee trip data associated with the business profile and allows organizations to review individual trips, locations, vehicle classes, and total rideshare/ride-hail expenses.

Why:
Safety, Security and privacy are paramount for both GSA Rideshare/Ride-hail vendors participating in the Blanket Purchase Agreement (BPA).

In order to ensure the platforms are safe we partnered with the GSA Chief Information Security Officer (OCISO) and GSA Senior Privacy Officer to develop custom security and privacy requirements for non-federal systems utilizing a modified version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

The GSA required the Rideshare/Ride-hail vendors to have a GSA OCISO-approved technical architecture in place that is inclusive of all IT components related to the system boundary such as logical access and connection flows to the Internet, external systems, Infrastructure as a Service (IaaS)/Platform as a Service (PaaS)/Software as a Service (SaaS), and to the Corporate network (as applicable) at a port, protocol, services level with related access/authentication flows for all user groups including vendor and customer user level and privileged level access.

Key Security Requirements and Deliverables -

GSA OCISO outlined key architecture and boundary scope review conditions expected of the Rideshare/Ride-hail vendors to include in their system security documentation. Detailed checklist items of the architecture requirements included:

- Information System Components and Boundary Considerations;
- Data Flow and Routing Paths; and
- Key Technical Security Considerations.

The Rideshare/Ride-hail's system security documentation must include control implementation statements that are clear, complete, concise, consistent, and describe who, what, when, where, and how the control is implemented. For GSA security teams, it is not sufficient for information system stakeholders to simply restate the control requirement. System security controls must specifically describe the vendor's implementation to allow a detailed understanding of the protection mechanisms supporting the control requirement(s). Included in the GSA's vendor security guidance documentation, the Rideshare/Ride-hail vendors are provided a Security Requirements Discussion Statements checklist to aid the vendor to document their security documentation completely and accurately.

November 2020

General Services Administration
Rideshare/Ride-hail Privacy and Security Overview

The GSA Rideshare/Ride-hail Program consists of GSA Privacy Office and OCISO security deliverables as described below.

Privacy Deliverables -

The GSA Privacy Office requires each Rideshare/Ride-hail vendor to prepare a Privacy Threshold Analysis (PTA) to confirm and document whether Personally Identifiable Information (PII) is within scope; and to determine which other categories of Controlled Unclassified Information (CUI) is stored, processed, or transmitted, via the system. The GSA Privacy Office provided the vendors with Guidance on Nonfederal Privacy Impact Assessment (PIA) that provides instructions on conducting a PIA for electronic information systems and collections in accordance with GSA CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices.

Vendor specific PIA documents can be found here:
https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems

Security Deliverables -

GSA OCISO has prescribed a set of security deliverables for each Rideshare/Ride-hail vendor to submit. Outlined below are the set of security deliverables.

- Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)
- System Security Plan (SSP) (based on GSA-customized NIST SP 800-171, Revision 2)
- Security Assessment Plan (SAP)
- Operating System Scans
- Web Application Scans
- Penetration Test Report (Recommended)
- Nonfederal System Test Cases
- Security Controls Assessment Report (SAR)
- Plan of Action and Milestones (POA&M)

For additional details about the GSA Security and Privacy Requirements for IT Acquisition Efforts:
https://www.gsa.gov/cdnstatic/Security_and_Privacy_Requirements_for_IT_Acquisition_Efforts_%5BCIO_IT_Security_09-48_Rev_5%5D_08-25-2020.pdf

For Additional Information:
Contact the GSA Rideshare/Ride-hail Program at rideshare.ridehail@gsa.gov.

November 2020