Department of Information Technology (WMATA-IT)

Incident Report: Rail Service Disruption June 16, 2017

Date: June 20, 2017

This document provides an overview of the events that led to the communication loss between the Advanced Information Management (AIM) system and the Remote Terminal Units (RTUs) on June 16, 2017 7:09 pm. It includes the chronological order of the events, analysis, and proposed corrective actions to minimize the risk of their reoccurrence.

Cause of Service Disruption – This disruption was caused by a known software defect PARP 6.1.1, PARP 6.1.4, PARP 6.1.5 hat causes network traffic to stop passing through the devices.

The software defect was a known product defect that was reported PARP 6.1.1, PARP 6.1.4, PARP 6.1.5 This report included a series of workaround recommendations to address the issue, including rebooting the firewalls regularly.

Sequence of Events - The following is a summary of sequence of events:

- At 19:09 the ROCC Operating support team noticed that RTUs were down.
- At 19:29 it was discovered that all workstations were down in PARP 6.1.1, PARP 6.1.4, PARP 6.1.5 Network Monitor. Code 34 was initiated.
- At 19:44 a bridge was opened for all stakeholders to track the progress of the incident and discuss possible workaround solutions.
- At 20:36 after a series of network and security analyses, it was discovered that the firewalls were not able to manage network traffic.
- At 20:38 the root cause is identified, and the decision was made to restart the firewalls. The reboot of the firewalls restored communications between the AIM system and the RTUs.
- At 20:57 full CTF firewall redundancy was restored.
- At 22:30 code 34 was lifted and the rail operation was back to normal.

Washington Metropolitan Area Transit Authority

Preliminary Observation and Analysis – Based on the initial observations from the data gathered, the factors attributed to this outage are PARP 6.1.5 As noted above, this was a known issue with a workaround solution released by the vendor.PARP 6.1.5

PARP 6.1.5

PARP 6.1.5