March 16, 2020

Mr. John Scano
Chief Development Officer (CDO)
Lookout, Inc.
Mobile Endpoint Security (MES)

Re: Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO)

Dear Mr. Scano:

The JAB of the Federal Risk and Authorization Management Program (FedRAMP) has completed the security authorization review of Lookout's Mobile Endpoint Security (MES), which leverages the Amazon East/West (AWS E/W) Infrastructure-as-a-Service (IaaS). Based on the Federal Information Processing Standard (FIPS) security categorization of Moderate and the FedRAMP Security Assessment Process[1], the JAB has determined that MES meets FedRAMP information security requirements, and is granted a FedRAMP P-ATO. Based on the third-party assessment conducted by EmeSec, and review by the JAB, there are no outstanding high vulnerabilities.

The P-ATO for MES will remain in effect for a length of time in alignment with Office of Management and Budget Circular A-130 as long as:

1. Lookout satisfies the requirement of implementing continuous monitoring activities in accordance with the Office of Management and Budget (OMB) *Memorandum M-19-02*, and as documented in FedRAMP's continuous monitoring requirements and the MES Continuous Monitoring Plan.
2. Lookout mitigates all open low and moderate POA&M action items, as agreed to in the Security Assessment Report (SAR).
3. Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal laws, guidelines, and policies.
4. Lookout takes action on all incidents in accordance with FedRAMP continuous monitoring requirements, including communication with Agency customers and the United States Computer Emergency Readiness Team (US-CERT).
5. AWS E/W P-ATO remains in effect.

[1] FedRAMP Security Assessment Process is available at www.fedramp.gov.

MES is delivered as a Software-as-a-Service (SaaS) offering using a multi-tenant public cloud computing environment. It is available to multiple organizations and agency clients.

The purpose of the Lookout MES solution is to protect mobile devices such as Apple and Android phones and tablets from phishing attempts, application malware, as well as device and network threats. This is done using data gathered from a large base of mobile devices and mobile applications. The data is then used as a baseline for cloud-based AI models that compare and analyze complex patterns that indicate known and novel threats, software vulnerabilities, risky mobile behaviors and configurations, and provides phishing protection. Once a problem is identified, the mobile user and the MES Console Administrator will be notified. Through the MES system the threat data can be shared with other commonly deployed enterprise solutions such as EMMs and SIEMs.

Federal Agencies are encouraged to make use of this FedRAMP P-ATO as a key element of their Authorization to Operate (ATO). The package associated with the MES FedRAMP P-ATO must be considered with the AWS E/W P-ATO. Agency customers must consider the aggregate risk for the two systems when granting an ATO. The JAB believes the MES FedRAMP Security Authorization Packages accurately document and clearly define the risk considerations.

Copies of the authorization packages are available for agency review in the FedRAMP Secure Repository. If you have any questions or comments regarding this P-ATO, please contact Ashley Mahan, FedRAMP Director, ashley.mahan@gsa.gov.

APPROVED:

X

Digitally signed by
WILMER.JOHN.W.III.1267975430
Date: 2020.04.17 10:03:07 -04'00'

Mr. Dana Deasy
Chief Information Officer
Department of Defense

X ELIZABETH A CAPPELLO

Digitally signed by ELIZABETH A
CAPPELLO
Date: 2020.04.14 08:02:24 -04'00'

Ms. Elizabeth A. Cappello
Chief Information Officer (Acting)
Department of Homeland Security

X

DocuSigned by:
David Shive
A3AF4284A2754F9...

Mr. David A. Shive
Chief Information Officer
General Services Administration