COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
October 25, 2017

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement from Chairman Darin LaHood (R-Ill.)

Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government

Chairman LaHood: Good morning and welcome to today's Oversight Subcommittee hearing, "Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government."

Today we intend to discuss and evaluate the cybersecurity posture of the federal government. Specifically, we will examine the concerns that this Committee has raised about the risks associated with using Kaspersky Lab's products on federal information technology (IT) systems, as well as actions that the Trump administration has taken in response to these concerns.

As part of today's hearing, we will hear from government and private sector cybersecurity experts about the potential risks that Kaspersky Lab products and services pose to agency IT systems. In doing so, we hope to find effective and efficient ways to improve agency practices related to the design, acquisition, development, modernization, use and performance of federal IT resources.

Kaspersky Lab is based in Moscow, Russia, and was founded in 1997 by Eugene Kaspersky. The company is one of the world's largest providers of cybersecurity software and services, including both consumer and enterprise solutions.

As early as 2015, reports began to surface alleging that Mr. Kaspersky maintained close ties to Russian spies. Not only was Mr. Kaspersky educated at a KGB-sponsored university, he also wrote code for the Soviet military.

In May of this year, the concerns surrounding Kaspersky Lab were brought to public light during a Senate Intelligence Committee hearing, where several intelligence community officials unanimously affirmed they would be uncomfortable using Kaspersky Lab's software and services. In June of this year, during this Committee's hearing on the WannaCry ransomware outbreak, our witnesses expressed similar concerns. The matter reached a tipping point in July, when the General Services Administration (GSA) announced the removal of Kaspersky Lab products from its pre-approved government contracts schedules.

On July 27, the Committee commenced its investigation of the matter, with Chairman Smith probing 22 federal departments and agencies on their use of Kaspersky Lab products and services.

Last month, the Trump administration took another step toward addressing the concerns surrounding Kaspersky when the Department of Homeland Security (DHS) issued Binding Operational Directive (BOD) 17-01, ordering all federal departments and agencies to remove Kaspersky Lab software from their systems within 90 days.

Mr. Kaspersky has been highly critical of the U.S. throughout this entire process, frequently arguing that no public evidence existed to support the concerns raised about his company.

Earlier this month, however, several prominent American news organizations published startling revelations that confirmed this Committee's gravest concerns: the Russian government has wielded Kaspersky's software as a tool for cyber-espionage.

This administration has been proactively remedying the Kaspersky situation. And we must continue to take steps to ensure that we do not repeat past mistakes.

To that end, I look forward to hearing from our expert witnesses about how Kaspersky became approved for use on federal systems, the policies and procedures that can be implemented to bolster the federal government's cybersecurity risk-management processes, and the actions that must be taken to ensure that federal systems remain secure against nefarious cyber actors.

###