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 Lamar Smith (R-Texas)

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

Chairman Smith: Cybersecurity breaches are so prevalent today that it is hard to keep track of them. Every news cycle seems to include a new major incident.

To address the federal government's cybersecurity weaknesses, the Committee hopes to bring H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, to the House floor for a vote.

Specific to Kaspersky Lab, new revelations regarding cyber-espionage continue to surface. This Committee has engaged in robust oversight of Kaspersky Lab, thanks to questions raised by Congressman Higgins during a hearing in June.

On July 27, 2017, this Committee requested all federal departments and agencies to disclose their use of Kaspersky Lab products.

This was less than a month after the U.S. General Services Administration (GSA) banned Kaspersky Lab products from its government-wide schedule contracts. However, we still have questions: Why was the software approved for government use? And was removing it from the approved GSA schedule sufficient to protect US interests?

I support this administration's subsequent actions. The interagency working group on cybersecurity has begun to address the problem.

On September 13, 2017, the Department of Homeland Security issued a government-wide order directing federal departments and agencies to identify and remove the company's products from use. In subsequent hearings, we will need to assess whether the federal government's response has been sufficient.

While once considered reputable, Kaspersky Lab, its founder and their Russian ties have created a significant risk to U.S. security. According to several media investigations, these connections have allowed Kaspersky Lab to be exploited not only by the Russian government but also by criminal hackers around the world.

Mr. Kaspersky's history and recent remarks have done little to alleviate these concerns.

As we move forward with this hearing and future hearings, we expect to uncover all aspects of Kaspersky Lab.

We are particularly interested in what led the previous administration to include Kaspersky Lab products on two GSA schedules. I look forward to the testimony of Mr. Shive, the GSA Chief Information Officer.

I am also interested in proactive steps GSA has taken to assist other departments and agencies in rooting out the presence of Kaspersky products on their systems.

Also, we need to better understand the recent news related to the breach of an NSA contractor's personal computer.

The threat Kaspersky Lab products present to the government has now been publicly identified and confirmed by the Israeli government.

I urge anyone with knowledge of potential risks to contact the Committee and share that information with us. We must be vigilant in addressing this wolf in sheep's clothing.

###