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

For Immediate Release
November 14, 2017

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

Statement from Darin LaHood (R-Ill.)

Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive

Chairman LaHood: Good morning and welcome to today's Oversight Subcommittee hearing: "Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive."

The purpose of this hearing is to examine and assess implementation of Department of Homeland Security (DHS) Binding Operational Directive 17-01, Removal of Kaspersky-Branded Products, by federal government departments and agencies.
This hearing marks the second time the committee has convened to examine the issues and concerns surrounding Kaspersky Lab.

On October 25, 2017, the committee examined the potential risks, vulnerabilities and threats posed to federal IT systems by Kaspersky software. During that hearing, we heard from experts about the specific nature of threats posed by Kaspersky, action the federal government has taken or plans to take to mitigate the threat and steps that could be taken to avoid similar threats in the future.

The Trump administration has taken steps to remediate the Kaspersky issue. In July of this year, the GSA removed Kaspersky from its government-wide contracts. Although this was a step in the right direction, it did not completely eliminate the threat.

On September 13, 2017, the administration took additional steps to harden the security of federal information systems against the Kaspersky threat when DHS issued Binding Operational Directive 17-01.

The directive requires federal departments and agencies to complete three consecutive phases of implementation. First, they must scan their systems to identify the use or presence of Kaspersky software. Second, they must develop an action plan for the removal and replacement of any Kaspersky software identified on their systems. Finally, they are required to implement their action plan, and must begin the process of removal and replacement.

Federal departments and agencies are also required to submit status reports to DHS as they implement each of the directive's three phases. The status reports provide data and information that is useful for assessing compliance with the directive, and for quantifying the pervasiveness of Kaspersky installations across federal systems, the extent of threats posed by the software and the complexities associated with complete removal.

Today, we will focus primarily on the status reports to guide our assessment of compliance with the directive. In doing so, we hope to learn whether agencies have complied with the first two phases of the directive, and whether any Kaspersky installations were found on federal systems.

Additionally, we hope to understand more about the specific action plans for removal and replacement of any identified Kaspersky installations, and DHS' anticipated timeline for full implementation of the directive.

Finally, we hope to learn about the directive's applicability to federal contractors. I want to thank Ms. Miller for being here to represent the Department of Defense. Annually, DOD spends approximately $30 billion on information technology. We are interested in whether the directive applies to DOD's contractors and, if so, are they complying? If not, what must be done to ensure that contractors take appropriate action to mitigate the Kaspersky threat?

I'm hopeful that our witnesses today can help us resolve these important questions, and better understand the next steps that must be taken to ensure the integrity, resilience and security of federal information systems.

Cybersecurity is a complex and evolving issue that affects U.S. national and economic security. We must remain diligent in our efforts to strengthen and secure federal systems, and our approaches to addressing cybersecurity issues must evolve to keep pace with ever-changing threats.

Bolstering the cybersecurity of federal information systems is among the committee's top priorities, and I am hopeful that our efforts here today will take us one step closer toward accomplishing this objective.

###