United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 24, 2017

The Honorable Elaine C. Duke
Acting Secretary
U.S. Department of Homeland Security
3801 Nebraska Avenue NW
Washington, DC 20528

Dear Madam Acting Secretary:

I am writing to inquire about the Binding Operational Directive (BOD) 17-01 that the Department of Homeland Security (DHS) issued to federal agencies regarding Kaspersky Lab products.

On September 13, 2017, DHS issued BOD 17-01 ordering all federal executive branch departments and agencies to take steps to remove Kaspersky Lab products from their systems.[1] Specifically, it "calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems."[2] I applaud the actions DHS is undertaking to remove Kaspersky Lab products from federal government systems.

Kaspersky products present a clear security threat to the U.S. As DHS noted in its statement, "The Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies."[3] Those relationships, coupled with the nature of how Kaspersky products work and the intersection with Russian law, pose significant national security concerns. In May, six national security officials testified before the Senate Select Committee on Intelligence and resoundingly said they would not be comfortable with Kaspersky Lab software on their systems.[4] In the BOD, DHS explained:

---

[1] DHS Statement on the Issuance of Binding Operational directive 17-01, DHS (Sept. 13, 2017) (www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01).

[2] *Id.*

[3] *Id.*

[4] Senate Select Committee on Intelligence, Hearing on Worldwide Threats (115th Cong.) (May 11, 2017).

> Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, which can be exploited by malicious cyber actors to compromise those information systems.... [Furthermore,] requirements under Russian law... allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security.[5]

In order to better understand the BOD and how it will be implemented, please provide answers to the following questions:

1. It is clear from testimony before the Senate Select Committee on Intelligence in May that administration officials were concerned about Kaspersky products for some time. Why did DHS wait to issue the BOD until September 13, four months after the intelligence committee hearing?

2. How many government systems are currently using Kaspersky products and how was that determination made?

3. What capability does DHS have to ascertain the full extent of federal agency use of Kaspersky products?

4. BODs do not apply to Defense Department or Intelligence Community systems, nor do they apply to "National Security Systems."[6] Which federal civilian systems are covered by the term National Security System?

5. How will DHS ensure compliance with the BOD within each agency?

6. How does DHS enforce BODs in other agencies?

7. Do federal information systems include non-federal systems used by contractors to connect to federal systems?

---

[5] DHS Statement on the Issuance of Binding Operational directive 17-01, DHS (Sept. 13, 2017) (www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01).

[6] Department of Homeland Security, *National Protection and Programs Directorate; Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses* (82 Fed. Reg. 43782) (Sept. 19, 2017).

8. How will DHS ensure compliance with contractors' systems that connect to federal information systems?

9. What should state and local governments be doing to ensure that their systems that connect with federal information systems are not using Kaspersky products?

10. What is DHS doing to disseminate information to the private sector and state and local governments that work with the federal government to raise awareness about Kaspersky products?

11. Please describe any repercussions the United States has experienced in response to DHS issuing the BOD ordering the removal of Kaspersky Lab products from U.S. government systems.

I request that you provide responses to these questions no later than November 14, 2017. If you or members of your staff have any questions about this request, please ask your staff to contact Julie Klein with my Committee at 202-224-2627. Please send any official correspondence relating to this request to Lucy Balcezak at Lucy_Balcezak@hsgac.senate.gov. Thank you for your attention to this matter.

Sincerely,

Claire McCaskill
Ranking Member

cc: Ron Johnson
Chairman