9110-9P-P

DEPARTMENT OF HOMELAND SECURITY

National Protection and Programs Directorate

Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Issuance of binding operational directive; procedures for responses; notice of availability.

SUMMARY: In order to safeguard Federal information and information systems, DHS has issued a binding operational directive to all Federal, executive branch departments and agencies relating to information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or affiliated companies. The binding operational directive requires agencies to identify Kaspersky-branded products (as defined in the directive) on Federal information systems, provide plans to discontinue use of Kaspersky-branded products, and, at 90 calendar days after issuance of the directive, unless directed otherwise by DHS in light of new information, begin to remove Kaspersky-branded products. DHS is also establishing procedures, which are detailed in this notice, to give entities whose commercial interests are directly impacted by this binding operational directive the opportunity to respond, provide additional information, and initiate a review by DHS.

DATES: Binding Operational Directive 17-01 was issued on September 13, 2017. DHS must receive responses from impacted entities on or before **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Submit electronic responses to Binding Operational Directive 17-01, along with any additional information or evidence, to *BOD.Feedback@hq.dhs.gov*.

SUPPLEMENTARY INFORMATION: The Department of Homeland Security ("DHS" or "the Department") has the statutory responsibility, in consultation with the Office of Management and Budget, to administer the implementation of agency information security policies and practices for information systems, which includes assisting agencies and providing certain government-wide protections. 44 U.S.C. 3553(b). As part of that responsibility, the Department is authorized to "develop[] and oversee[] the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidance developed by the Director [of the Office of Management and Budget] and [certain] requirements of [the Federal Information Security Modernization Act of 2014.]" 44 U.S.C. 3553(b)(2). A binding operational directive ("BOD") is "a compulsory direction to an agency that (A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; [and] (B) [is] in accordance with policies, principles, standards, and guidelines issued by the Director[.]" 44 U.S.C. 3552(b)(1). Agencies are required to comply with these directives. 44 U.S.C. 3554(a)(1)(B)(ii).

OVERVIEW OF BOD 17-01

In carrying out this statutory responsibility, the Department issued BOD 17-01, titled "Removal of Kaspersky-Branded Products." The text of BOD 17-01 is reproduced in the next section of this document.

Binding Operational Directive 17-01 may have adverse consequences for the commercial interests of AO Kaspersky Lab or other entities. Therefore, the Department will provide entities whose commercial interests are directly impacted by BOD 17-01 the opportunity to respond to the BOD, as detailed in the Administrative Process for Responding to Binding Operational Directive 17-01 section of this notice, below.

TEXT OF BOD 17-01

Binding Operational Directive BOD-17-01

Original Issuance Date: September 13, 2017

Applies to: All Federal Executive Branch Departments and Agencies

FROM: Elaine C. Duke, Acting Secretary, Department of Homeland Security

CC: Mick Mulvaney, Director, Office of Management and Budget

SUBJECT: Removal of Kaspersky-Branded Products

A binding operational directive is a compulsory direction to Federal, executive branch, departments and agencies for purposes of safeguarding Federal information and information systems. 44 U.S.C. 3552(b)(1). The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA"). 44 U.S.C. 3553(b)(2). Federal agencies are required to comply with these DHS-developed directives. 44 U.S.C. 3554(a)(1)(B)(ii). DHS binding operational directives do not apply to statutorily defined "National Security Systems" nor to certain systems operated by the Department of Defense and the Intelligence Community. 44 U.S.C. 3553(d)-(e).

Background: DHS, in consultation with interagency partners, has determined that the risks presented by Kaspersky-branded products justify issuance of this Binding Operational Directive.

Definitions:

- "Agencies" means all Federal, executive branch, departments and agencies. This directive does not apply to statutorily defined "National Security Systems" nor to certain systems operated by the Department of Defense and the Intelligence Community. 44 U.S.C. 3553(d)-(e)
- "Kaspersky-branded products" means information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates, including Kaspersky Lab North America, Kaspersky Lab, Inc., and Kaspersky Government Security Solutions, Inc. (collectively, "Kaspersky"), including those identified below.

Kaspersky-branded products currently known to DHS are: Kaspersky Anti-Virus; Kaspersky Internet Security; Kaspersky Total Security; Kaspersky Small Office Security; Kaspersky Anti Targeted Attack; Kaspersky Endpoint Security; Kaspersky Cloud Security (Enterprise); Kaspersky Cybersecurity Services; Kaspersky Private Security Network; and Kaspersky Embedded Systems Security.

This directive does not address Kaspersky code embedded in the products of other companies. It also does not address the following Kaspersky services: Kaspersky Threat Intelligence and Kaspersky Security Training.

- "Federal information system" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

Required Actions: All agencies are required to:

1. Within 30 calendar days after issuance of this directive, identify the use or presence of Kaspersky-branded products on all Federal information systems and provide to DHS a report that includes:

a. A list of Kaspersky-branded products found on agency information systems. If agencies do not find the use or presence of Kaspersky-branded products on their Federal information systems, inform DHS that no Kaspersky-branded products were found.

b. The number of endpoints impacts by each product, and

c. The methodologies employed to identify the use or presence of the products.

2. Within 60 calendar days after issuance of this directive, develop and provide to DHS a detailed plan of action to remove and discontinue present and future use of all Kaspersky-branded products beginning 90 calendar days after issuance of this directive. Agency plans must address the following elements in the attached template[1] at a minimum:

a. Agency name

b. Point of contact information, including name, telephone number, and email address

c. List of identified products

d. Number of endpoints impacted

e. Methodologies employed to identify the use or presence of the products

f. List of Agencies (components) impacted within Department

g. Mission function of impacted endpoints and/or systems

h. All contracts, service-level agreements, or other agreements your agency has entered into with Kaspersky

i. Timeline to remove identified products

j. If applicable, FISMA performance requirements or security controls that product removal would impact, including but not limited to data loss/leakage prevention,

[1] The template for agency plans has not been reproduced in the *Federal Register*, but is available (in electronic format) from DHS upon request.

network access control, mobile device management, sandboxing/detonation chamber, website reputation filtering/web content filtering, hardware and software whitelisting, vulnerability and patch management, anti-malware, anti-exploit, spam filtering, data encryption, or other capabilities

k. If applicable, chosen or proposed replacement products/capabilities

l. If applicable, timeline for implementing replacement products/capabilities

m. Foreseeable challenges not otherwise addressed in this plan

n. Associated costs related to licenses, maintenance, and replacement (please coordinate with agency Chief Financial Officers)

3. At 90 calendar days after issuance of this directive, and unless directed otherwise by DHS based on new information, begin to implement the agency plan of action and provide a status report to DHS on the progress of that implementation every 30 calendar days thereafter until full removal and discontinuance of use is achieved.

DHS Actions:

- DHS will rely on agency self-reporting and independent validation measures for tracking and verifying progress.
- DHS will provide additional guidance through the Federal Cybersecurity Coordination, Assessment, and Response Protocol (the C-CAR Protocol) following the issuance of this directive.

Potential Budgetary Implications: DHS understands that compliance with this BOD could result in budgetary implications. Agency Chief Information Officers (CIOs) and procurement officers should coordinate with the agency Chief Financial Officer (CFO), as appropriate.

DHS Point of Contact: Binding Operational Directive Team[2]

Attachment: BOD 17-01 Plan of Action Template[3]

ADMINISTRATIVE PROCESS FOR RESPONDING TO BINDING OPERATIONAL DIRECTIVE 17-01

The Department will provide entities whose commercial interests are directly impacted by BOD 17-01 the opportunity to respond to the BOD, as detailed below:

- The Department has notified Kaspersky about BOD 17-01 and outlined the Department's concerns that led to the decision to issue this BOD. This correspondence with Kaspersky is available (in electronic format) to other parties whose commercial interests are directly impacted by BOD-17-01, upon request. Requests must be directed to *BOD.Feedback@hq.dhs.gov*.
- If it wishes to initiate a review by DHS, by **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**, Kaspersky, and any other entity that claims its commercial interests will be directly impacted by the BOD, must provide the Department with a written response and any additional information or evidence supporting the response, to explain the adverse consequences, address the Department's concerns, or mitigate those concerns.
- The Department's Assistant Secretary for Cybersecurity and Communications, or another official designated by the Secretary of Homeland Security ("the Secretary"), will review the materials relevant to the issues raised by the entity, and will issue a recommendation to the Secretary regarding the matter. The Secretary's decision will be

[2] The email address to be used by Federal agencies to contact the DHS Binding Operational Directive Team has not been reproduced in the Federal Register.

[3] The template for agency plans has not been reproduced in the *Federal Register*, but is available (in electronic format) from DHS upon request.

communicated to the entity in writing by **[INSERT DATE 85 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

- The Secretary reserves the right to extend the timelines identified above.

Elaine C. Duke
Secretary of Homeland Security (Acting)
Department of Homeland Security
[FR Doc. 2017-19838 Filed: 9/18/2017 8:45 am; Publication Date: 9/19/2017]