Acting Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Binding Operational Directive *BOD-17-01*

Original Release 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"). Id.* § 3553(b)(2). *Federal agencies are required to comply with these DHS-developed directives. Id.* § 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. Id.* § 3553(d)-(e).

Background:

DHS, in consultation with interagency partners, has determined that the risks presented by Kaspersky-branded products justify the 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 impacted 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 at a minimum:
    a. Agency name
    b. Point of contact information, including name, telephone, 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, 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, FNR.BOD@hq.dhs.gov. All agency reports and plans related to this directive shall be sent to this address.

Attachment:

1. BOD 17-01 Plan of Action Template