Dated: September 11, 2017.

Ira S. Reese,

Executive Director, Laboratories and Scientific Services Directorate.

[FR Doc. 2017–19863 Filed 9–18–17; 8:45 am]

BILLING CODE 9111–14–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Waiver of Compliance With Navigation Laws; Hurricanes Harvey and Irma

AGENCY: Office of the Secretary, Department of Homeland Security.

ACTION: Notice.

On September 8, 2017, I issued a limited waiver of the Jones Act upon the recommendation of the Department of Energy and at the request of the Department of Defense.[1] Hurricane Harvey striking the U.S. Gulf Coast has resulted in severe disruptions in both the midstream and downstream sectors of the oil supply system. Some refineries and pipeline networks are shut-in or running at reduced rates. Thus, conditions exist for a continued shortage of energy supply in areas predicted to be affected by Hurricane Irma. In light of this, the Department of Energy has recommended that the Department of Homeland Security waive the requirements of the Jones Act in the interest of national defense to facilitate the transportation of the necessary volume of petroleum products through September 22, 2017. Furthermore, the Department of Defense has requested a waiver of the Jones Act in the interest of national defense through September 22, 2017, commencing immediately.

The Jones Act, 46 United States Code (U.S.C.) 55102, states that a vessel may not provide any part of the transportation of merchandise by water, or by land and water, between points in the United States to which the coastwise laws apply, either directly or via a foreign port unless the vessel was built in and documented under the laws of the United States and is wholly owned by persons who are citizens of the United States. Such a vessel, after obtaining a coastwise endorsement from the U.S. Coast Guard, is ''coastwise-qualified.'' The coastwise laws generally apply to points in the territorial sea, which is defined as the belt, three nautical miles wide, seaward of the territorial sea baseline, and to points located in internal waters, landward of the territorial sea baseline.

The navigation laws, including the coastwise laws, can be waived under the authority provided by 46 U.S.C. 501. The statute provides in relevant part that on request of the Secretary of Defense, the head of an agency responsible for the administration of the navigation or vessel-inspection laws shall waive compliance with those laws to the extent the Secretary considers necessary in the interest of national defense. 46 U.S.C. 501(a).

For the reasons stated above, and in light of the request from the Department of Defense and the concurrence of the Department of Energy, I am exercising my authority to waive the Jones Act through September 22, 2017, commencing immediately, to facilitate movement of refined petroleum products, including gasoline, diesel, and jet fuel, to be shipped from New York, New Jersey, Delaware, Maryland, Pennsylvania, New Mexico, Texas, Louisiana, Mississippi, Alabama, and Arkansas to Florida, Georgia, South Carolina, North Carolina, Virginia, West Virginia, and Puerto Rico. This waiver applies to covered merchandise laded on board a vessel through and including September 22, 2017.

Executed this 12th day of September, 2017.

Elaine C. Duke,

Acting Secretary of Homeland Security.

[FR Doc. 2017–19902 Filed 9–18–17; 8:45 am]

BILLING CODE 9111–14–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 November 3, 2017.

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.

[1] Published in the **Federal Register** at 82 FR 43248 (Sept. 14, 2017).

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, network access control, mobile device management, sandboxing/detonation chamber, Web site 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]

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

[2] The email address to be used by Federal agencies to contact the DHS Binding Operational

Continued

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 November 3, 2017, 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 communicated to the entity in writing by December 13, 2017.
- 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 9–18–17; 8:45 am]

BILLING CODE 9910–9P–P

DEPARTMENT OF THE INTERIOR

Bureau of Indian Affairs

[178A2100DD/AAKC001030/ A0A501010.999900 253G]

Proclaiming Certain Lands as Reservation for the Jamestown S'Klallam Tribe of Washington

AGENCY: Bureau of Indian Affairs, Interior.

ACTION: Notice of reservation proclamation.

SUMMARY: This notice informs the public that the Acting Assistant Secretary—Indian Affairs proclaimed approximately 267.29 acres, more or less, an addition to the reservation of the Jamestown S'Klallam Tribe on July 21, 2017.

FOR FURTHER INFORMATION CONTACT: Ms. Sharlene M. Round Face, Bureau of Indian Affairs, Division of Real Estate Services, 1849 C Street NW., MS–4642–MIB, Washington, DC 20240, Telephone: (202) 208–3615.

SUPPLEMENTARY INFORMATION: This notice is published in the exercise of authority delegated by the Secretary of the Interior to the Assistant Secretary—Indian Affairs by part 209 of the Departmental Manual.

A proclamation was issued according to the Act of June 18, 1934 (48 Stat. 986; 25 U.S.C. 5110) for the land described below. The land was proclaimed to be the Jamestown S'Klallam Reservation for the Jamestown S'Klallam Tribe, Clallam County, State of Washington.

Jamestown S'Klallam Reservation for the Jamestown S'Klallam Tribe

14 Parcels—Legal Description Containing 267.29 Acres, More or Less

Tribal Tract Number: 129–T1004

Legal description containing 5.090 acres, more or less.

That portion of Lot 28 of Keeler's Sunrise Beach, as recorded in Volume 4 of plats, page 46, records of Clallam County, Washington, lying between the Northeasterly right of way line of the Chicago, Milwaukee, St. Paul and Pacific Railway and the Northeasterly right of way line of the present existing State Highway No. 9 and bounded on the Southeasterly end by the Northerly right of way line of the existing Old Olympic Highway;

Also, that portion of the Northeast Quarter of the Southeast Quarter of Section 34, Township 30 North, Range 3 West, W.M., Clallam County, Washington, lying between the Northeasterly right of way line of the Chicago, Milwaukee, St. Paul and Pacific Railway and the Northeasterly right of way line of the present existing State Highway No. 9.

Excepting therefrom that portion of the Northeast Quarter of the Southeast Quarter of said Section 34, Township 30 North, Range 3 West, W.M., Clallam County, Washington, described as follows starting and ending at the point identified as the *True Point Of Beginning:*

Commencing at the East Quarter Corner of said Section 34; thence North 87°42′55″ West, a distance of 317.69 feet along the North Line of the said Northeast Quarter of the Southeast Quarter to a point lying on the Northeasterly right-of-way line of the abandoned Chicago, Milwaukee, St. Paul and Pacific Railroad and the *True Point Of Beginning;* Thence South 49°56′33″ East along said right-of-way line, a distance of 112.08 feet to a point lying on a tangent curve, concave Southwesterly and having a radius of 2914.62 feet; Thence Southeasterly along said curve through a central angle of 05°25′36″, an arc length of 276.05 feet; Thence leaving said curve North 85°53′09″ West, a distance of 33.08 feet; Thence North 46°13′33″ West, a distance of 372.52 feet to the North line of said Northeast Quarter of the Southeast Quarter; Thence South 87°42′55″ East along said North line, a distance of 13.65 feet to the *True Point of Beginning.* As described in Boundary Line Agreement recorded May 29, 2007 as Recording No. 2007–1201967. Said instrument is a re-recording of Auditor's File No. 2007–1200907 and 2007–1201792. Situate in the County of Clallam, State of Washington. Containing 5.090 acres, more or less.

Tribal Tract Number: 130–T1169

Legal description containing 30.36 acres, more or less.

Parcel A: The East Half of the Southeast Quarter of the Northeast Quarter and the Southeast Quarter of the Northeast Quarter of the Northeast Quarter in Section 11, Township 30 North, Range 4 West, W.M., Clallam County, Washington.

Parcel B: An easement for ingress, egress and utilities over a 30 foot easement along the East Line of the Northeast Quarter of the Northeast Quarter of the Northeast Quarter in Section 11, Township 30 North, Range 4 West, W.M., Clallam County, Washington. Containing 30.36 acres, more or less.

Tribal Tract Number: 129–T1003

Legal description containing 5.00 acres, more or less.

Parcel A: That portion of the South Half of the Northeast Quarter of the Northeast Quarter of Section 26, Township 30 North, Range 4 West, W.M., Clallam County, Washington, described as Parcel 1 as delineated on Survey recorded in Volume 4 of Surveys, page 25, under Auditor's File No. 497555, situate in Clallam County, State of Washington.

Parcel B: An easement for ingress, egress and utilities over, under and

---

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.