AMENDMENT TO RULES COMM. PRINT 118–10
OFFERED BY MS. PORTER OF CALIFORNIA

Add at the end of subtitle B of title XVIII the following:

SEC. 1824. REPORT ON IRANIAN INTERNET CENSORSHIP.

(a) In general.—The Secretary of the Treasury and the Secretary of State shall jointly submit to Congress a report regarding Iranian internet censorship and applicable United States licensing requirements. Such report shall the following:

(1) An assessment of the Iranian Government’s ability to impose internet shutdowns, censor the internet, and track Iranian dissidents, labor organizers, political activists, or human rights defenders inside Iran through targeted digital surveillance or other digital means.

(2) An assessment of the impact of General License D-2, issued on September 23, 2022, on the availability of private communications tools inside Iran, including encryption tools to assist the people of Iran in circumventing digital surveillance by the Iranian Government.
(3) A determination of whether additional updates to General License D-2 or other licenses are needed to keep up with the pace of technology and ensure that United States restrictions do not unintentionally inhibit the flow of vital communication tools to the people of Iran, including cloud technology, hardware, software, and services incident to personal communications, including set-top boxes (STB), satellites, and web developer tools.

(4) A strategy to ensure that resources are available for digital rights experts to study Iran’s online repression and identify opportunities to counter it.

(5) A strategy to prevent the Government of Iran from acquiring or developing tools that could be exploited against activists, including facial recognition software.

(b) FORM.—The report required pursuant to subsection (a) shall be submitted in unclassified form but may include a classified annex if such annex is provided separately from such unclassified version.

(c) DEFINITION.—In this section, the term “targeted digital surveillance” means the use of items or services that enable an individual or entity (with or without the knowing authorization of the product’s owner) to detect,
monitor, intercept, collect, exploit, preserve, protect, trans-
mit, retain, or otherwise gain access to the communica-
tions, sensitive or protected information, work product,
browsing data, research, identifying information, location
history, or online or offline activities of other individuals,
organizations, or entities.