AMENDMENT TO RULES COMM. PRINT 118–10
OFFERED BY MS. WASSERMAN SCHULTZ OF
FLORIDA

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

SEC. 1859. THREAT ASSESSMENT ON CYBER HARASSMENT

AND ITS USE BY TERRORISTS AND FOREIGN
MALICIOUS ACTORS.

(a) IN GENERAL.—The Under Secretary for Intel-
ligence and Analysis of the Department of Homeland Se-
curity shall develop and disseminate a threat assessment
regarding the use of cyber harassment, including doxing,
by terrorists and foreign malicious actors.

(b) COORDINATION.—The threat assessment devel-
oped pursuant to subsection (a)—

(1) shall be developed in coordination with the
Privacy Office of the Department of Homeland Se-
curity and the Office for Civil Rights and Civil Lib-
erties of the Department of Homeland Security; and

(2) may be informed by existing products, as
appropriate.

(c) REQUIREMENTS.—The threat assessment devel-
oped pursuant to subsection (a) shall include—
(1) an overview of cyber harassment tactics, techniques, and procedures used by terrorists and foreign malign actors;

(2) a list of notable incidents of cyber harassment by terrorists and foreign malign actors;

(3) a review of the threat posed by cyber harassment, including tactics, techniques, and procedures not currently identified as in use by terrorists and foreign malign actors, but representing a vulnerability based on the common practices of such actors, as well as a summary of the terrorist and foreign malign actors most likely to adapt to use of such tactics, techniques, and procedures; and

(4) an overview of cyber harassment typologies and methodologies that may inform risk indicators of relevance to State, local, Tribal, and Federal law enforcement in identifying cyber harassment that may be indicative of terrorist or foreign malign actor involvement.

(d) DISSEMINATION AND PUBLICATION.—The Under Secretary shall—

(1) not later than 180 days after the date of the enactment of this Act, submit the threat assessment to Congressional committees of jurisdiction; and
(2) consistent with the protection of classified
and confidential unclassified information—

(A) disseminate the threat assessment de-
veloped under this section with State, local, and
Tribal law enforcement officials, including offi-
cials who operate within State, local, and re-
gional fusion centers through the Department
of Homeland Security State, Local, and Re-
gional Fusion Center Initiative established in
accordance with section 210A of the Homeland

(B) ensure a version of the assessment is
published on the Department’s website no later
than 30 days following dissemination to Con-
gress.

(e) DEFINITIONS.—For the purposes of this section:

(1) CYBER HARASSMENT.—The term “cyber
harassment” means electronic communication that
harasses, torments, threatens, or terrorizes a target.

(2) DOXING.—The term “doxing” means to
knowingly publish the personally identifiable infor-
mation of another individual, without the individ-
ual’s consent and with the intent to—

(A) threaten, intimidate, harass, or stalk
any person;
(B) facilitate another to threaten, intimidate, harass, or stalk any person;

(C) incite or facilitate the commission of a crime of violence against any person; or

(D) place any person in reasonable fear of death or serious bodily injury.

(3) PERSONALLY IDENTIFIABLE INFORMATION.—The term “personally identifiable information” means—

(A) any information that can be used to distinguish or trace an individual’s identity, such as name, prior legal name, alias, mother’s maiden name, social security number, date or place of birth, address, phone number, or biometric data;

(B) any information that is linked or linkable to an individual, such as medical, financial, education, consumer, or employment information, data, or records; or

(C) any other sensitive private information that is linked or linkable to a specific identifiable individual, such as gender identity, sexual orientation, or any sexually intimate visual depiction.
(4) TERRORISTS.—The term “terrorists” refers to—

(A) any designated Foreign Terrorist Organization (FTO);

(B) any group or actor supporting activities that may be covered by section 2331(5) of title 18, United States Code; and

(C) any group or actor investigated by the intelligence community pursuant to the intelligence review represented by “Domestic Violent Extremism Poses Heightened Threat in 2021”, 01 March 2021.

(5) FOREIGN MALIGN ACTOR.—The term “foreign malign actor” refers to any foreign adversary entities covered by section 5322(e)(2) of the National Defense Authorization Act for Fiscal Year 2020 (50 U.S.C. 3059(e)(2)).

(f) RULES OF CONSTRUCTION.—For purposes of construing this section, the following shall apply:

(1) AUTHORITIES.—Nothing in this section may be construed to confer any authority, including law enforcement authority, beyond that which is authorized under existing law.

(2) CONSTITUTIONAL PROTECTIONS.—Nothing in this section may be construed to prohibit any con-
stitutionally protected speech, expressive conduct or activities (regardless of whether compelled by, or central to, a system of religious belief), including the exercise of religion protected by the First Amendment and peaceful picketing or demonstration. The Constitution does not protect speech, conduct, or activities consisting of planning for, conspiring to commit, or committing an act of violence.

(3) PRIVACY.—Nothing in this section may be construed to preempt or conflict with existing Federal privacy laws, except in circumstances listed herein.

(4) FREE EXPRESSION.—Nothing in this section may be construed to allow prosecution based solely upon an individual’s expression of racial, religious, political, or other beliefs or solely upon an individual’s membership in a group advocating or espousing such beliefs.