AMENDMENT NO. 2612

By FRANKEN

To:

S. 754

Page(s) 3

Purpose: To improve the definitions of cybersecurity threat and cyber threat indicator.

IN THE SENATE OF THE UNITED STATES—114th Cong., 1st Sess.

Viz:

1 Beginning on page 3, strike line 21 and all that follows through page 5, line 8, and insert the following:

2 system that is reasonably likely to result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

3 (B) EXCLUSION.—The term “cybersecurity threat” does not include any action that solely
involves a violation of a consumer term of service or a consumer licensing agreement.

(6) CYBER THREAT INDICATOR.—The term “cyber threat indicator” means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the harm caused by an incident, including a description of the information
exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such information is not otherwise prohibited by law; or