AMENDMENT TO THE RULES COMMITTEE PRINT OF H.R. 3523

OFFERED BY M__. _____

Page 14, after line 14 insert the following:

''(1) AVAILABILITY.—The term 'availability' means ensuring timely and reliable access to and use of information.

Page 15, strike lines 1 through 25 and insert the following:

''(2) CONFIDENTIALITY.—The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

''(3) CYBER THREAT INFORMATION.—

''(A) IN GENERAL.—The term 'cyber threat information' means information directly pertaining to—

''(i) a vulnerability of a system or network of a government or private entity;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity

or any information stored on, processed on, or transiting such a system or network;

''(iii) efforts to degrade, disrupt, or destroy a system or network of a government or private entity; or

''(iv) efforts to gain unauthorized access to a system or network of a government or private entity, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity.

''(B) EXCLUSION.— Such term does not include information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

''(4) CYBER THREAT INTELLIGENCE.—

''(A) IN GENERAL.—The term 'cyber threat intelligence' means intelligence in the possession of an element of the intelligence community directly pertaining to—

''(i) a vulnerability of a system or network of a government or private entity;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or any information stored on, processed on, or transiting such a system or network;

''(iii) efforts to degrade, disrupt, or destroy a system or network of a government or private entity; or

''(iv) efforts to gain unauthorized access to a system or network of a government or private entity, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity.

''(B) EXCLUSION.— Such term does not include intelligence pertaining to efforts to gain unauthorized access to a system or network of a government or private entity that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Page 16, strike line 5 and all that follows through page 17, line 2, and insert the following:

''(5) CYBERSECURITY PURPOSE.—

''(A) IN GENERAL.—The term 'cybersecurity purpose' means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

''(i) a vulnerability of a system or network;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

''(iii) efforts to degrade, disrupt, or destroy a system or network; or

''(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

''(B) EXCLUSION.— Such term does not include the purpose of protecting a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

''(6) CYBERSECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'cybersecurity system' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

''(i) a vulnerability of a system or network;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

''(iii) efforts to degrade, disrupt, or destroy a system or network; or

''(iv) efforts to gain unauthorized access to a system or network, including to

gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

''(B) EXCLUSION.— Such term does not include a system designed or employed to protect a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Page 17, after line 2 insert the following:

''(7) INTEGRITY.—The term 'integrity' means guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

☒