# AMENDMENT TO THE RULES COMMITTEE PRINT OF H.R. 3523 OFFERED BY MR. SCHIFF OF CALIFORNIA

Page 1, beginning on line 1, strike ''The Director of National Intelligence'' and insert ''The Secretary of Homeland Security, in consultation with the Director of National Intelligence,''.

Page 8, after line 10, insert the following new paragraph:

''(4) PRIVACY AND CIVIL LIBERTIES.—

''(A) REQUIREMENT FOR POLICIES AND PROCEDURES.—The Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Secretary of Defense, and privacy and civil liberties experts, shall develop and periodically review policies and procedures governing the receipt, retention, use, and disclosure of cyber threat information received in accordance with paragraph (1). Such policies and procedures shall—

''(i) minimize the impact on privacy and civil liberties, consistent with the need

to protect a system or network from cybersecurity threats and mitigate cybersecurity threats;

''(ii) reasonably limit the receipt, retention, use and disclosure of cybersecurity threat indicators associated with specific persons consistent with the need to carry out the responsibilities of this Act, including establishing a process for the timely destruction of cybersecurity threat indicators that are received pursuant to this section that do not reasonably appear to be related to protecting a system or network from cybersecurity threats and mitigating cybersecurity threats;

''(iii) include requirements to safeguard cybersecurity threat indicators that can be used to identify specific persons from unauthorized access or acquisition; and

''(iv) protect the confidentiality of cybersecurity threat information associated with specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be

used for protecting a system or network against cybersecurity threats or mitigating against cybersecurity threats.

''(B) ADOPTION OF POLICIES AND PROCEDURES.—The head of a department or agency of the Federal Government receiving cyber threat information in accordance with paragraph (1) shall adopt and comply with the policies and procedures developed under subparagraph (A).

''(C) REVIEW BY THE ATTORNEY GENERAL.—Not later than 1 year after the date of the enactment of the Cyber Intelligence Sharing and Protection Act, the policies and procedures developed under subparagraph (A) shall be reviewed and approved by the Attorney General.

''(D) PROVISION TO CONGRESS.—The policies and procedures issued under subparagraph (A) and any amendments to such policies and procedures shall be provided to Congress.

Page 9, strike line 6 and all that follows through page 10, line 10, and insert the following new subsection:

''(c) FEDERAL GOVERNMENT USE OF INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the head of a department or agency of the Federal Government may only use, retain, or further disclose cyber threat information received in accordance with subsection (b)(1) in order to protect a system or network from cybersecurity threats.

''(2) EXCEPTIONS.—The head of a department or agency of the Federal Government may disclose cyber threat information received in accordance with subsection (b)(1) to—

''(A) another head of a department or agency of the Federal Government if the information discloses a specific and immediate threat to the national security of the United States or is considered foreign intelligence information (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)); or

''(B) a law enforcement entity if the information appears to pertain to—

''(i) an imminent danger of death or serious physical injury to any person; or

''(ii) an imminent danger of serious harm to a child under the age of 13.

''(3) NON-DELEGABLE AUTHORITY.—The head of a department or agency of the Federal Government may not delegate the authority provided under paragraph (2).

''(4) DISCLOSURE OF INFORMATION.—Any disclosure of information under this subsection shall be made only as permitted under the procedures developed by the Secretary of Homeland Security and approved by the Attorney General under subsection (b)(4).

Page 15, strike line 1 and all that follows through page 17, line 2, and insert the following:

''(2) CYBERSECURITY PROVIDER.—The term 'cybersecurity provider' means a non-governmental entity that provides goods or services intended to be used for a cybersecurity purposes.

''(3) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' means the purpose of detecting, preventing, or mitigating a cybersecurity threat.

''(4) CYBERSECURITY SYSTEM.—The term 'cybersecurity system' means a system designed or employed to detect, prevent, or mitigate a cybersecurity threat.

''(5) CYBERSECURITY THREAT.—The term 'cybersecurity threat' means any action that may re-

sult in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of a system or network or information that is stored on, processed by, or transiting a system or network.

''(6) CYBERSECURITY THREAT INFORMATION.—The term 'cybersecurity threat information' means information—

''(A) that may be indicative of or describe—

''(i) malicious reconnaissance, including anomalous patterns of communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(ii) a method of defeating a technical control;

''(iii) a technical vulnerability;

''(iv) a method of defeating an operational control;

''(v) a method of causing a user with legitimate access to a system or network or information that is stored on, processed by, or transiting a system or network to unwit-

tingly enable the defeat of a technical control or an operational control;

''(vi) malicious cyber command and control;

''(vii) the actual or potential harm caused by an incident, including information exfiltrated as a result of subverting a technical control when it is necessary in order to identify or describe a cybersecurity threat;

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

''(ix) any combination thereof; and

''(B) from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to the cybersecurity threat.

''(7) CYBER THREAT INTELLIGENCE.—The term 'cyber threat intelligence' means cybersecurity threat information in the possession of an element of the intelligence community.

''(8) MALICIOUS CYBER COMMAND AND CONTROL.—The term 'malicious cyber command and

control' means a method for remote identification of, access to, or use of, a system or network or information that is stored on, processed by, or transiting a system or network associated with a known or suspected cybersecurity threat.

''(9) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring a system or network for the purpose of discerning technical vulnerabilities of the system or network, if such method is associated with a known or suspected cybersecurity threat.

''(10) OPERATIONAL CONTROL.—The term 'operational control' means a security control for a system or network that primarily is implemented and executed by people.

''(11) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of a system or network or information that is stored on, processed by, or transiting a system or network that is intended to ensure the confidentiality, integrity, or availability of that system.

''(12) TECHNICAL VULNERABILITY.—The term 'technical vulnerability' means any attribute of hard-

ware or software that could enable or facilitate the defeat of a technical control.

Page 17, beginning on line 17, strike ''Director of National Intelligence'' and insert ''Secretary of Homeland Security''.

Page 18, beginning on line 2, strike ''Secretary of Homeland Security'' and insert ''Director of National Intelligence''.