AMENDMENT TO THE RULES COMMITTEE PRINT OF H.R. 3523 OFFERED BY MS. JACKSON LEE OF TEXAS

Page 9, after line 5, insert the following:

''(c) CYBERSECURITY OPERATIONAL ACTIVITY.—

''(1) IN GENERAL.—In receiving information authorized to be shared with the Federal Government under this section, the Secretary of Homeland Security is authorized, notwithstanding any other provision of law, to acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on Federal systems and to deploy countermeasures with regard to such communications and system traffic for cybersecurity purposes provided that the Secretary certifies that—

''(A) such acquisitions, interceptions, and countermeasures are reasonable necessary for the purpose of protection Federal systems from cybersecurity threats;

''(B) the content of communications will be collected and retained only when the communication is associated with known or reasonably

suspected cybersecurity threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with such threats;

''(C) information obtained pursuant to activities authorized under this subsection will only be retained, used or disclosed to protect Federal systems from cybersecurity threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed; and

''(D) notice has been provided to users of Federal systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic.

''(2) CONTRACTS.— The Secretary may enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities that provide electronic communication or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic consistent with paragraph (1).

''(3) PRIVILEGED COMMUNICATIONS.—No otherwise privileged communication obtained in accordance with, or in violation of, this section shall lose its privileged character.

''(4) POLICIES AND PROCEDURES.— The Secretary of Homeland Security shall establish policies and procedures that—

''(A) minimize the impact on privacy and civil liberties, consistent with the need to protect Federal systems and critical information infrastructure from cybersecurity threats and mitigate cybersecurity threats;

''(B) reasonably limit the acquisition, interception, retention, use, and disclosure of communications, records, system traffic, or other information associated with specific persons consistent with the need to carry out the responsibilities of this section, including establishing a process for the timely destruction on recognition of communications, records, system traffic, or other information that is acquired or intercepted pursuant to this section that does not reasonably appear to be related to protecting Federal systems and critical information

infrastructure from cybersecurity threats and mitigating cybersecurity threats;

''(C) include requirements to safeguard communications, records, system traffic, or other information that can be used to identify specific persons from unauthorized access or acquisition; and

''(D) protect the confidentiality of disclosed communications, records, system traffic, or other information associated with specific persons to the greatest extent practicable and require recipients of such information to be informed that the communications, records, system traffic, or other information disclosed may only be used for protecting information systems against cybersecurity threats, mitigating against cybersecurity threats, or law enforcement purposes when the information is evidence of a crime that has been, is being, or is about to be committed, as specified by the Secretary.

Page 14, after line 24, insert the following:

''(2) COUNTERMEASURE.—The term 'countermeasure' means an automated action with defensive intent to modify or block data packets associated with electronic or wire communications, internet

traffic, program code, or other system traffic transiting to or from or stored on an information system to counteract a cybersecurity threat.''.