5. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE JACKSON LEE OF TEXAS OR HER DESIGNEE, DEBATABLE FOR 10 MINUTES

11

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

1 suspected cybersecurity threat, and communica-
2 tions and system traffic will not be subject to
3 the operation of a countermeasure unless asso-
4 ciated with such threats;
5 "(C) information obtained pursuant to ac-
6 tivities authorized under this subsection will
7 only be retained, used or disclosed to protect
8 Federal systems from cybersecurity threats,
9 mitigate against such threats, or, with the ap-
10 proval of the Attorney General, for law enforce-
11 ment purposes when the information is evidence
12 of a crime which has been, is being, or is about
13 to be committed; and
14 "(D) notice has been provided to users of
15 Federal systems concerning the potential for ac-
16 quisition, interception, retention, use, and dis-
17 closure of communications and other system
18 traffic.
19 "(2) CONTRACTS.— The Secretary may enter
20 into contracts or other agreements, or otherwise re-
21 quest and obtain the assistance of, private entities
22 that provide electronic communication or
23 cybersecurity services to acquire, intercept, retain,
24 use, and disclose communications and other system
25 traffic consistent with paragraph (1).

1 "(3) PRIVILEGED COMMUNICATIONS.—No oth-
2 erwise privileged communication obtained in accord-
3 ance with, or in violation of, this section shall lose
4 its privileged character.
5 "(4) POLICIES AND PROCEDURES.— The Sec-
6 retary of Homeland Security shall establish policies
7 and procedures that—
8 "(A) minimize the impact on privacy and
9 civil liberties, consistent with the need to pro-
10 tect Federal systems and critical information
11 infrastructure from cybersecurity threats and
12 mitigate cybersecurity threats;
13 "(B) reasonably limit the acquisition,
14 interception, retention, use, and disclosure of
15 communications, records, system traffic, or
16 other information associated with specific per-
17 sons consistent with the need to carry out the
18 responsibilities of this section, including estab-
19 lishing a process for the timely destruction on
20 recognition of communications, records, system
21 traffic, or other information that is acquired or
22 intercepted pursuant to this section that does
23 not reasonably appear to be related to pro-
24 tecting Federal systems and critical information

1 infrastructure from cybersecurity threats and
2 mitigating cybersecurity threats;
3 "(C) include requirements to safeguard
4 communications, records, system traffic, or
5 other information that can be used to identify
6 specific persons from unauthorized access or ac-
7 quisition; and
8 "(D) protect the confidentiality of dis-
9 closed communications, records, system traffic,
10 or other information associated with specific
11 persons to the greatest extent practicable and
12 require recipients of such information to be in-
13 formed that the communications, records, sys-
14 tem traffic, or other information disclosed may
15 only be used for protecting information systems
16 against cybersecurity threats, mitigating
17 against cybersecurity threats, or law enforce-
18 ment purposes when the information is evidence
19 of a crime that has been, is being, or is about
20 to be committed, as specified by the Secretary.

Page 14, after line 24, insert the following:

21 "(2) COUNTERMEASURE.—The term 'counter-
22 measure' means an automated action with defensive
23 intent to modify or block data packets associated
24 with electronic or wire communications, internet

1 traffic, program code, or other system traffic
2 transiting to or from or stored on an information
3 system to counteract a cybersecurity threat.".