AMENDMENT TO THE RULES COMMITTEE PRINT FOR H.R. 1731
OFFERED BY MR. HURD OF TEXAS

Add at the end the following:

SEC. ___ PROTECTION OF FEDERAL INFORMATION SYSTEMS.

(a) In General.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

“SEC. 233. AVAILABLE PROTECTION OF FEDERAL INFORMATION SYSTEMS.

“(a) In General.—The Secretary shall deploy and operate, to make available for use by any Federal agency, with or without reimbursement, capabilities to protect Federal agency information and information systems, including technologies to continuously diagnose, detect, prevent, and mitigate against cybersecurity risks (as such term is defined in the second section 226) involving Federal agency information or information systems.

“(b) Activities.—In carrying out this section, the Secretary may—

“(1) access, and Federal agency heads may disclose to the Secretary or a private entity providing
assistance to the Secretary under paragraph (2), in-
formation traveling to or from or stored on a Fed-
eral agency information system, regardless of from
where the Secretary or a private entity providing ass-
stance to the Secretary under paragraph (2) ac-
resses such information, notwithstanding any other
provision of law that would otherwise restrict or pre-
vent Federal agency heads from disclosing such in-
formation to the Secretary or a private entity pro-
viding assistance to the Secretary under paragraph
(2);

“(2) enter into contracts or other agreements,
or otherwise request and obtain the assistance of,
private entities to deploy and operate technologies in
accordance with subsection (a); and

“(3) retain, use, and disclose information ob-
tained through the conduct of activities authorized
under this section only to protect Federal agency in-
formation and information systems from
cybersecurity risks, or, with the approval of the At-
torney General and if disclosure of such information
is not otherwise prohibited by law, to law enforce-
ment only to investigate, prosecute, disrupt, or oth-
otherwise respond to—
“(A) a violation of section 1030 of title 18, United States Code;

“(B) an imminent threat of death or serious bodily harm;

“(C) a serious threat to a minor, including sexual exploitation or threats to physical safety; or

“(D) an attempt, or conspiracy, to commit an offense described in any of subparagraphs (A) through (C).

“(c) CONDITIONS.—Contracts or other agreements under subsection (b)(2) shall include appropriate provisions barring—

“(1) the disclosure of information to any entity other than the Department or the Federal agency disclosing information in accordance with subsection (b)(1) that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk; and

“(2) the use of any information to which such private entity gains access in accordance with this section for any purpose other than to protect Federal agency information and information systems against cybersecurity risks or to administer any such contract or other agreement.
“(d) LIMITATION.—No cause of action shall lie against a private entity for assistance provided to the Secretary in accordance with this section and a contract or agreement under subsection (b)(2).”.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to cybersecurity recruitment and retention) the following new item:

“Sec. 233. Available protection of Federal information systems.”.