Amendment to the Rules Committee Print

of H.R. 3523

Offered by Mr. Thompson of Mississippi

Page 18, after line 15 insert the following:

(c) Privacy and Civil Liberties Oversight.—

(1) Policies and Procedures.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security, in consultation with the Director of National Intelligence and privacy and civil liberties stakeholders, shall develop and periodically review policies and procedures governing the acquisition, interception, retention, use, and disclosure of communications, records, system traffic, or other information associated with specific persons by officers, employees, and agents of the Federal Government in connection with activities authorized under this Act or the amendments made by this Act. Such policies and procedures shall—

(A) minimize the impact on privacy and civil liberties, consistent with the need to mitigate cybersecurity threats;

(B) reasonably limit the acquisition, interception, retention, use, and disclosure of com-
munications, records, system traffic, or other information associated with specific persons consistent with the need to carry out the responsibilities of this Act and the amendments made by this Act, including establishing a process for the timely redaction and destruction of communications, records, system traffic, or other information that is acquired or intercepted pursuant to this Act or the amendments made by this Act that does not reasonably appear to be related to protecting against cybersecurity threats and mitigating cybersecurity threats;

(C) require reasonable efforts to remove information that can be used to identify a specific individual, using automated means if technically feasible, upon initial receipt of the information;

(D) 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

(E) protect the confidentiality of disclosed communications, records, system traffic, or other information associated with specific per-
sons 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 of Homeland Security.

(2) ATTORNEY GENERAL APPROVAL.—The Attorney General shall review and approve the policies and procedures developed under paragraph (1).