Summary of S. 2519, the National Cybersecurity Protection Act of 2014

S. 2519 would codify the National Cybersecurity and Communications Integration Center at the Department of Homeland Security and the Center's existing cybersecurity responsibilities. The legislation (as amended) was negotiated with the Committee on Homeland Security and includes provisions that are similar to H.R. 3696, the Cybersecurity and Critical Infrastructure Protection Act of 2014, which is co-sponsored by Chairman McCaul and Ranking Member Bennie Thompson and passed the House under suspension of the rules.

Cyber attacks continue to grow and are a major threat to our nation's economic and national security. Within the federal government, the Department of Homeland Security is responsible for working with the private sector to help protect the nation's critical infrastructure from cyber threats and overseeing the security of federal networks. At the center of DHS' cybersecurity is the National Cybersecurity and Communications Integration Center ("NCICC" or "Center"). The NCICC is a round-the-clock operations center where government, private sector, and other stakeholders work together on cybersecurity and other matters. Codification of this center will help DHS carry out its cybersecurity mission more effectively and efficiently.

The Homeland Security and Governmental Affairs Committee reported the legislation with strong bipartisan support. The Congressional Budget Office estimates that implementing the legislation would not result in a significant cost.

The legislation would codify the NCCIC's existing role as a civilian interface for the cross-sector sharing of cybersecurity information. The legislation would also codify the Center's existing responsibilities to: conduct analysis of cybersecurity risks and incidents; provide, upon request, incident response and technical assistance; and recommend security and resilience measures to enhance cybersecurity. The legislation would direct the Center to ensure its activities are timely, actionable, and risk-based; coordinated across critical infrastructure sectors; and compliant with privacy and civil liberties laws. Under the legislation, the Center would continue to be composed of representatives from Federal and non-Federal entities.

The legislation would also require DHS to work with federal and non-Federal partners to develop and exercise cyber incident response plans to address cybersecurity risks to critical infrastructure. The bill would also put greater management and oversight attention on cyber breaches by improving notification of breaches to the public and to Congress.