S.1869, The Federal Cybersecurity Enhancement Act of 2015

Federal networks are under continuous attack in cyberspace by sophisticated actors and nation states. There were nearly 70,000 information security incidents on federal government networks in fiscal year 2014, up 15 percent from fiscal year 2013. Many federal agencies struggle to keep pace—over the last several years foreign adversaries have stolen tens of millions of Americans' sensitive data as a result of insufficient cybersecurity practices. The consequences of the cyber attack on the Office of Personnel Management, for example, will not likely be fully known for years.

The Carper-Johnson Federal Cybersecurity Enhancement Act (FCEA) would improve federal network security by by mandating the deployment of cybersecurity best practices at agencies and authorizing and accelerating the use of the Department of Homeland Security's (DHS) cyber intrusion detection and prevention system across the federal government.

FCEA would require Federal agencies to implement best practices in cybersecurity—practices that could have prevented or reduced the impact of major breaches like those at the Office of Personnel Management and Internal Revenue Service. For example, the bill mandates several cybersecurity controls—including two-factor authentication and encryption for sensitive systems. *It also would require DHS and the Office of Management and Budget (OMB) to conduct a comprehensive assessment to hunt down and remove intruders in federal networks.* Implementing these cybersecurity best practices would complement and enhance security provided by the intrusion detection and prevention system authorized by the bill. *FCEA would provide individual agencies and Congress, the public, and the President greater insight into agencies' cybersecurity as well as their enforcement tools to ensure best practices in cybersecurity are followed.*

FECA authorizes DHS's intrusion detection and prevention system, EINSTEIN. EINSTEIN analyzes federal agencies' network traffic to identify and stop cyber threats. Although the Administration has attempted to deploy EINSTEIN at agencies across the federal government, the system is not yet available to all federal agencies and less than half are using the intrusion prevention capability. This is in part because of legal uncertainty about DHS's authorities to deploy the program and agencies' authority to participate.

FCEA would speed up adoption of EINSTEIN across the government by clarifying legal authorities for the program and mandating agency adoption. It would advance the system's capabilities by requiring DHS to update EINSTEIN with advanced cyber technologies, including commercial tools. *The bill would also improve privacy protections for the system and increase transparency and accountability of the EINSTEIN program by requiring annual status reports.* Finally, to ensure continued oversight of the program, FCEA would include reporting requirements from DHS and OMB and a seven year sunset.