The Senate Cybersecurity Protection Act of 2019

"The personal accounts and devices of government officials can contain information that is useful for our adversaries to target, either directly or indirectly, these officials and the organizations with which they are affiliated."
– The Hon. Dan Coats, Director of National Intelligence, April 2018.

This bill will permit the Senate Sergeant at Arms (SAA) to provide voluntary cybersecurity assistance to protect the personal accounts and devices of Senators and certain Senate staff.

Russia's actions in 2016 highlighted how the personal email accounts of senior officials can be weaponized against our democracy. Indeed, every single email account that was hacked and leaked in 2016 was either a personal or campaign account.

Currently, the Sergeant at Arms asserts that it may not lawfully use funds authorized for securing the Senate's information technology to protect the personal devices or accounts of Senators or Senate staff. The SAA has refused to provide Senators and staff with assistance or advice, even after Google told them their personal accounts were targeted by foreign government hackers.

What the bill does

This bill permits the SAA to provide opt-in, voluntary assistance to Senators and certain Senate staff to secure their personal devices (laptops, desktops, cell phones, tablets, and other Internet-connected devices) and accounts (email, text messaging, cloud computing, social media, telephone, residential Internet, health care, and financial services)

No Senator or staffer is required by this bill to receive cybersecurity assistance of any kind.

Anyone receiving help must first sign an annual memorandum of understanding that:
1) Specifies the accounts or devices for which the Sergeant at Arms will provide security; and
2) Describes the rights and responsibilities of each party relating to the provision of security.

Which staff are eligible for protection under this bill?

Any Senate staffer is eligible for protection, providing that their supervising Senator or the head of their office determines the staffer is "highly vulnerable to cyber attacks and hostile information collection activities because of the position of the individual."

What precedent is there for using official resources to protect personal devices & accounts?

Section 1645 of the 2017 National Defense Authorization Act permits the Department of Defense to provide personal device cybersecurity assistance to officials whom the Secretary "determines to be highly vulnerable to cyber attacks and hostile information collection activities because of the positions occupied by such personnel in the Department."

The Senate Select Committee on Intelligence approved an intelligence authorization bill in 2018 with language that would similarly protect intelligence community personnel.