Secure and Interoperable Government Collaboration Technology Act

The Secure and Interoperable Government Collaboration Technology Act will enhance national security, improve government efficiency, and save taxpayer dollars by requiring the government to purchase collaboration technology that is interoperable, end-to-end encrypted, and built on open standards. Collaboration technology includes tools for text-based messaging, voice and video calling, and live document editing like Microsoft Teams, Slack, and Google Docs.

Phone networks don't require their customers to use the same network just to make a call. Not so with internet-based collaboration technologies: if one user is on Teams and the other on Zoom, there's no way for the two products to talk to each other. For the Federal government, where dozens of agencies use different collaboration technologies, this lack of interoperability hurts the efficiency of collaboration processes, from video calling to scheduling.

The Secure and Interoperable Government Collaboration Technology Act would ensure the federal government is procuring and using collaboration technology that is based on interoperable, secure standards – meaning an employee from an agency using Teams could call someone from an agency using Zoom, or send a message to another agency that uses Slack. It also requires the use of end-to-end encryption technology, which is critically important to protect government communications from snooping by foreign adversaries, but has been unevenly adopted by the major video calling platforms used by government agencies. It also would require collaboration software used by the government to allow agencies to comply with federal record-keeping requirements – a growing concern as an increasing share of agency business is conducted through new collaborative software systems.

Collaboration technology providers who sell to the government should not be locking users into their walled product gardens using proprietary data standards. Government agencies, including the National Security Agency, Marines, and Navy, have endorsed the use of standards-based technology and security practices like end-to-end encryption – it's time for these principles to be reflected in the collaboration technology the federal government procures and uses.

The Secure Government Collaboration Technology Act would –

- Require the General Services Administration (GSA) to create a list of collaboration technology features used by the federal government, and the National Institute of Standards and Technology (NIST) to identify a set of interoperable standards, requirements, and guidance for each of these collaboration technology features.
- Require that, to the fullest extent possible, the standards use end-to-end encryption and other technologies to protect U.S. government communications from foreign surveillance.
- Require that collaboration technologies are designed to allow agencies to comply with federal record-keeping requirements.

- Four years after NIST identifies the standards, require that collaboration technology procured by the federal government be capable of communicating using the identified standards, so that it's interoperable with other products used within the government.
- Tasks the Department of Homeland Security with conducting cybersecurity reviews of collaboration technology products widely used by the federal government.
- Create a GSA and Office of Management and Budget working group to produce biennial reviews of collaboration tech used by the federal government to suggest additions or improvements to the standards.