DEPARTMENT OF ADMINISTRATIVE SERVICES

Senate Bill No. 1191

An Act Prohibiting the Use of a Certain Application, Software, and Programs on State Government Devices and Requiring Minimum Security Standards and Annual Audits of Such Devices

Testimony of the Department of Administrative Services (DAS)

Committee on Government Administration and Elections

March 10, 2023

Good morning, Senator Flexer, Representative Blumenthal, Senator Sampson, Representative Mastrofrancesco, and distinguished members of the Government Administration and Elections Committee. My name is Mark Raymond, and I am the Chief Information Officer for the State of Connecticut. In my role, I also oversee the Department of Administrative Services' Bureau of Information Technology Solutions (BITS).

At the outset, I want to thank you for your attention to this important topic.

Protecting the systems, networks and data of the state is a matter of critical importance. It is also a landscape that is continually changing. The risks and threats that face Connecticut are real and increasing, but we are vigilant in addressing them through the collaborative work of our state agencies and federal, municipal, and other partners.

Given that work, DAS believes that this legislation duplicates many of the existing controls already in place within our statutes, regulations, and administrative policies and procedures to ensure security standards are applied consistently across state government.

To provide additional information about our state cybersecurity initiatives, we have prepared and attached a summary document for your consideration.

Once again, thank you for raising this issue and for the opportunity to share background about our ongoing work in this space.

Connecticut Cybersecurity Initiatives and Programs

Statewide Cybersecurity Committee

- Subcommittee of the Advisory Council of the Division of Emergency Management and Homeland Security at the Department of Emergency Services and Public Protection (DESPP/DEMHS), meets monthly.
- Participants sign a Non-Disclosure Agreement, and include state, tribal, local, federal, and private sector partners.
- Co-chaired by DAS Chief Information Officer and DEMHS Deputy Commissioner. Emerging issues and best practices at local, state, and national levels are discussed.

Regional Emergency Planning Teams (REPTs)

- DEMHS has five REPTs made up of CEOs/representatives from each municipality in the region, as well as representatives from each public safety discipline organized in Emergency Support Functions (fire, law enforcement, public health, emergency management, public works, communications, etc.)
- At both the state and local level, cybersecurity is now identified as ESF 17, and each REPT has an ESF 17 committee, led by a municipal cybersecurity subject matter expert.

Free Municipal Cyber Assessments

- The Secretary of the State Elections Division, DEMHS and the CT National Guard have been collaborating on an initiative to provide municipalities with a cyber assessment free of charge, conducted by the National Guard.
- Funding for this initiative is from SOTS elections funds and federal homeland security grants.
- Currently, 48 towns have participated in the assessment, which takes about 90 minutes, and 48 towns are scheduled for an assessment. Additional federal funding has been set aside to complete assessment for all towns.

Federal Cybersecurity Grant

- FEMA and the federal DHS Cybersecurity and Infrastructure Security Agency (CISA) have released a federal Cybersecurity Grant aimed largely at improving cybersecurity at the municipal level, including rural areas.
- DEMHS and DAS' Bureau of Information Technology Solutions (BITS) are coordinating the implementation of the grant in CT.
- Established a Cybersecurity Grant Planning Committee - made up of local, state, and federal representatives and subject matter experts who are working to identify the types of cybersecurity enhancements eligible under the grant.
- The results of the municipal cyber assessments are helping to identify gaps in cybersecurity at the municipal level to create a “menu” of eligible projects.

Cyber Disruption Response Plan(s)

- The State has created several plans to assist in state and local cyber disruption response, including the state Cyber Disruption Response Plan and a cyber incident response plan which was sent as a template to municipalities. Outlines, among other issues, how a municipality or other affected organization or entity can report incidents and request assistance, if possible.
- DEMHS will be drafting an ESF 17 Cybersecurity Annex to the Local Emergency Operations Plan template to assist municipalities in maintaining cybersecurity.

CT Intelligence Center (CTIC)

- State's Intelligence Center, which includes a cybersecurity intelligence analyst (vacancy currently being filled), as well as federal and state cybersecurity partners, who analyze trends, coordinate assistance, and share information with municipal, state, federal partners.
- CTIC partners include the FBI, CISA and the CT National Guard.
- CTIC provides a monthly briefing to the Statewide Cybersecurity Committee, and is an information-sharing hub for state, local, federal, and private sector partners.

Other Initiatives

- DESPP Division of State Police includes a Cyber Crimes Unit that investigates cyber-crimes.
- DEMHS has hired a local-focused cybersecurity trainer who will be providing training to municipalities across the state.
- DAS provides security awareness training for all state employees helping to reduce cybersecurity risk by highlighting risks and mitigation options.
- DAS maintains an online, CT Cyber Library. On this site includes the State's Cyber Security Strategic Plan, last updated in March 2022.
- DAS provides 24x7 monitoring of security events related to the state's network.
- Cyber Yankee exercise run by CT National Guard and takes a regional approach to critical infrastructure incident exercise. 2023 will be second event run in CT.
- State's annual exercise of the State Response Framework and Unified Command often includes cyber components as a part of the exercise.
- DAS rolled out advanced endpoint detection and mitigation tools to all state executive branch agencies in 2022. These tools prevent ransomware and other advanced malware attacks.
- The State of CT and most CT municipalities participate in the Multi-State Information Sharing and Analysis Center (MS-ISAC). This organization provide free and low-cost cybersecurity services to government entities. Membership is free to public sector entities.
- Federal CISA provides free and low-cost cybersecurity services to state and local governments. This includes weekly scans of networks for external vulnerabilities and more intensive cybersecurity assessments.
- DAS, PURA and DEMHS conduct annual, voluntary reviews of the cybersecurity protections of CT utility providers.
- OPM develops and publishes IT Policies, in collaboration with DAS that cover important topics such as Acceptable Use Policy, Personal Device Use Policy and Network Security Policy.