State of Connecticut Cybersecurity Strategy

Point of contact: Jeff Brown, Chief Information Security Officer jeff.brown@ct.gov

Version 3.14 Mar 09, 2022

Introduction

In January 2020, Governor Lamont outlined a new focus for the State of Connecticut: To become the first all-digital government. The biennial budget enacted in June 2020 established a new Digital Government Services team within the Department of Administrative Services. Agencies have also delivered on significant digital government initiatives – DMV online services, business.ct.gov, DRS myConnect, SOTS Business Registration Services, COVID-19 related applications, data and websites to name a few. The Lamont administration continues to support the vision of Digital Government through legislative actions, investments and strong executive commitment.

As part of the "State of Connecticut Information and Telecommunications Strategic Plan for Fiscal Year 2022," the State of Connecticut (the State) established cybersecurity as one of its top strategic goals that helps guide the alignment and prioritization of strategic IT capital investments. This strategic plan outlines complementary goals including IT Optimization, Accelerating Digital Government Services and Improving Cybersecurity Statewide.

In support of the IT Strategic Plan, the State of Connecticut Cybersecurity Strategy (The Strategy) helps prepare our state, local and tribal governments for today's digital challenges by increasing our cybersecurity preparedness. Cyberattacks are more complex, frequent and damaging than ever before. This means it is critical for all states, including Connecticut, to develop a comprehensive strategy to mitigate cybersecurity risk. In response to this need, The State is outlining its cybersecurity strategy in this document.

The aim of the cybersecurity strategy is to protect State information assets; enable cybersecurity operations; ensure cybersecurity education; and ensure collaboration across both public and private sectors. Achieving these goals involves understanding the threat landscape and the dynamics of cybersecurity risk, including both external and internal cybersecurity threats.

Executive Summary

In January 2020, Governor Ned Lamont outlined a new focus for the State of Connecticut: to become the first all-digital state government. The Lamont administration continues to support the vision of Digital Government through legislative actions, capital investments and strong executive commitment. A key objective of the State Cybersecurity Strategy is to support and enable all forms of Digital Government and provide a framework for business resiliency and operational risk management.

The State cybersecurity strategy provides a roadmap for cyber risk mitigation for State, local and tribal levels of government in Connecticut and offers a plan to help protect critical infrastructure, networks, data, and technology systems. The cybersecurity strategy focuses on protecting against threats, regardless of their source, which includes nation-states, terrorists, criminal groups and human error. The strategy outlines four basic goals and objectives, including: ensuring secure state information systems, increasing outreach to public and private sectors, addressing the cyber skills shortage and preparing for increased cybersecurity attacks with resiliency planning.

Risk Appetite Statement

The **Playbook: Enterprise Risk Management for the Federal Government** defines risk appetite as "the amount of risk an organization is willing to accept on a broad level in pursuit of its objectives given consideration of costs and benefits." Without closely considering risk appetite, an organization may take risks greater than what may be appropriate to achieve strategic objectives. A clearly expressed and well-communicated risk appetite statement provides guidance on the amount of risk that is acceptable in the pursuit of our objectives and can help policymakers make more informed decisions.

The State operates in an overall low risk appetite range. The State has no tolerance for security exposures that could result in risk to employee and citizen health and safety or exposure of citizen private data. While there may be some smaller segments of state and local government that value speed and innovation more highly, the State government operates at an overall low risk tolerance. As such, the State will tolerate low-to-moderate risks related to running the day-to-day operations of other IT systems and networks that do not involve public safety or citizen data.

State Cybersecurity Strategic Goals and The Importance of Cybersecurity

Companies, government agencies, nonprofits, and others who conduct business in Connecticut are required by state law to disclose known electronic breaches of Connecticut residents' personal information to the State's Attorney General's office. Data released to Hearst Connecticut Media Group by the state Attorney General's office shows 1,062 breaches affected roughly 546,000 Connecticut residents in 2020. Cybersecurity threats continue to grow year-over-year.

State government handles many critical services, including healthcare, education and public safety. The State will protect sensitive data and critical infrastructure by implementing a comprehensive cybersecurity strategy based on potential risk impact. Technology advances and additional risks pose a constant challenge to cybersecurity professionals, especially those in state government, who must secure vast amounts of data from both intentional attacks and from unintentional misuse.

The Strategy helps inform and influence funding decisions for cybersecurity objectives across State, local and tribal entities. Defining a strategy helps the State understand a more holistic view of risk and better focus and align scarce security resources with the business objectives in the State.

There are four major objectives of the Cybersecurity Strategy. These are:

- Ensure enhanced security for State systems by building a best-in-class, centralized cybersecurity program.
- Increase public outreach and information sharing of cyber threats.
- Address the cybersecurity skills shortage.
- Prepare for cyber-attacks through resiliency planning.

The following section discusses each objective, and the actions required to support achieving these objectives in detail.

Objective 1: Ensure enhanced security for state systems by building a best-in-class, centralized cybersecurity program under the executive branch of government. The mission of this group is to build a best-in class cybersecurity program and a resilient technology infrastructure that supports Digital Government efforts and the constituents of Connecticut.

Background

While Objective 1 applies directly to State government and agencies, we recommend all local, tribal, educational institutions and quasi-agencies consider these controls for their own purposes.

The State is building a new information technology organization to better serve our employees and the citizens of Connecticut. The Department of Administrative Services (DAS) established a centralized technology organization, the Bureau of Information Technology Solutions (BITS), capable of delivering IT solutions and supporting State agencies and the citizens of Connecticut.

DAS/BITS is accountable for delivering the technology operations of state-owned IT systems. The centralized technology organization will be better capable of supporting agency needs. Centralized resources also enhance the State's cybersecurity posture by leveraging required skill sets across all agencies while providing a holistic view of threats against state government systems.

To support achieving this goal, the State is taking the following actions:

Actions:

- **Designate a Chief Information Security Officer (CISO) role with overall responsibility for the cybersecurity program.** The State of Connecticut established the formal CISO role in March 2020. The CISO is the cybersecurity executive responsible for the design and implementation of the overall State Cybersecurity program and for setting the strategic direction of the DAS/BITS cybersecurity organization. The ultimate accountability for the support and resourcing of the cybersecurity program resides with the acting governor. The Lamont administration announced a $11 Million investment for enhanced cybersecurity efforts on July 15th, 2021.

- **Design and implement a cybersecurity program to support State government employees, State IT resources and Digital Government initiatives.** On March 17th, 2021, Governor Lamont announced the launch of an information technology optimization process within State Government. The IT Optimization process brings best practices to all state agencies, provides flexibility cross-training employees, and ensures there is a pool of specialized experts to serve state agencies. The CISO shall have responsibility for building and maintaining the unified enterprise State cybersecurity program and supporting team of qualified security professionals. Bringing statewide information technology teams together through the IT Optimization efforts into one, collaborative organization helps identify and react to cybersecurity incidents faster, brings everyone onto streamlined platforms, and ultimately helps protect private information.

- **Align cybersecurity activities with established guidelines and standards.** With the passing of Public Act 21-119, the State of Connecticut encourages the private sector to adopt an industry-appropriate cybersecurity framework. A framework serves as a system of standards, guidelines, and best practices to manage cybersecurity risk and prioritizes a flexible, repeatable and cost-effective approach to promote the protection and resilience of technology systems. The State will adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework to help lay the groundwork for strong cybersecurity policy and governance and begin to adopt relevant principles and practices of a Zero Trust security model, as outlined by NIST.

- **Leverage Federal funding and grant opportunities to support enhancements to the cybersecurity program.** A significant portion of network traffic for education, municipal and State government flows through the Connecticut Education Network (CEN). This provides an opportunity to deploy enhanced security controls at a point that can benefit many government and education entities within the state. The State will investigate the possibility of leveraging Federal grants that may grow or enhance the existing security controls provided through CEN.

- **Continue to grow and enhance a culture of cybersecurity by implementing a robust training program for all state employees.** The weakest point for the security of an organization is often its personnel. The State will create a culture of cybersecurity awareness by leveraging enhanced training and awareness materials, running simulated phishing and tabletop exercises and supporting specific training for high-risk roles, including system administrators.

- **Protect State elections infrastructure and processes.** Protect State elections infrastructure and processes. In conjunction with the Secretary of the State, the State shall support Federal, State and local election security programs by coordinating with partners, including the Department of Homeland Security (DHS) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) and the Federal Bureau of Investigation (FBI) to protect various components of the overall election process.

- **Protect the State from risks introduced by third parties and supply chain risk by establishing a third-party risk management program.** This program will consider the sensitivity of data, network connectivity and the overall criticality of third-party and supply chain risk to the State of Connecticut. To achieve this objective, the State will examine compliance and procurement policies and procedures to ensure that State vendors can demonstrate compliance with State cybersecurity and privacy requirements.

Objective 2: Increase public sector outreach and information sharing about cyber threats.

The state fusion center, known as the Connecticut Intelligence Center (CTIC), centralizes Homeland Security Intelligence gathering in Connecticut. Fusion centers operate nationwide to receive, analyze, gather, and share threat-related information. Located within the Division of Emergency Management and Homeland Security (DEMHS) at the Department of Emergency Services and Public Protection (DESPP), CTIC includes a co-located team of Federal, State, and Local partners. These partners include State Agency Intelligence Liaison Officers, including from the Department of Correction, the Judicial Department, and the Connecticut Military Department; the Federal Bureau of Investigation (FBI), DHS Intelligence and Analysis, the Transportation Security Administration, the High Intensity Drug Trafficking Area (HIDTA) program, representatives from Fire/EMS and; Regional Intelligence Liaison Officers representing local law enforcement agencies from across the state. CTIC collects, analyzes and disseminates criminal, terrorism, and cyber related intelligence to its partners throughout the state which includes public and private sector entities.

The State shall accomplish the outreach objective by partnering with other government organizations including the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI.

Actions:

- **Continue an ongoing monthly statewide Cybersecurity Committee meeting that includes federal, state, and local partners, private industry and academia.** Cybersecurity expertise often lies across multiple government and industry sectors and academic institutions, and many of these experts would likely be eager to contribute to state cybersecurity efforts and policy. The State shall continue and expand this forum, which is currently occurring on a monthly cadence. Furthermore, cyber threat intelligence briefings are provided by CTIC at each of the meetings.

- **Continue encouraging MS-ISAC membership for eligible entities across the state.** This information sharing organization provides many resources that both municipal and state government can leverage, often at no or limited cost. There are currently 185 Connecticut members of the MS-ISAC, including municipalities and other eligible organizations, including public school districts.

- **Share relevant cyber threat information with public and private entities.** Sharing shall take place via the monthly State Cybersecurity Committee, through public service announcements and as finished products from CTIC. Continue to improve the communication and response processes to cyber threats across state agencies by ensuring the timely dissemination of threat information and automated response processes, where applicable.

- **Ensure that citizens have access to cybersecurity information that improves their personal security and privacy.** That State shall maintain and update an Internet landing page at https://portal.ct.gov/connecticut-cybersecurity-resource-page with relevant and timely information and cybersecurity awareness.

- **Leverage CTIC as a central cyber and threat intelligence and information sharing function for the state.** CTIC will continue its mission of collecting, analyzing and disseminating criminal, terrorism and cyber related intelligence to its partners in Connecticut, to the national fusion center network, and to its federal partners in the intelligence community.

- **Encourage reporting of cyber incidents in Connecticut to CTIC.** This information will help CTIC to provide better intelligence and more timely warnings to entities within Connecticut and potentially prevent future attacks. The information will also be used to increase situational awareness for the federal government and other fusion centers in the country and identify trends. The information could also be used by law enforcement in criminal investigations.

Objective 3: Address the cybersecurity skills shortage.

The cybersecurity training market has grown rapidly; however, there are still not enough qualified cybersecurity professionals available to fill open positions. The shortage of cybersecurity skills leaves both public and private entities at risk by leaving critical security positions left unfilled.

An objective of the cybersecurity strategy is to improve education opportunities and training in cybersecurity. Actions include:

Actions:

- **Partner with educational institutions to support cybersecurity training and education programs within the state.** The State will establish a cybersecurity internship program that will allow students to gain real-world experience during their studies, which is crucial in today’s employment market. It could also provide career opportunities in public service.

- **Ensure adequate resources within State government to train and develop employee knowledge of cybersecurity issues and responsibilities.** Training and awareness efforts must be part of an overall security and awareness program that considers discrepancies in cybersecurity knowledge.

Objective 4: Prepare for cyber-attacks through resiliency planning.

Cybersecurity attacks are inevitable in an always connected digital world. Therefore, it’s important that organizations carry out incident response planning and preparation activities. The State will take part in risk assessments and incident response planning activities. Response planning is an important way to prepare for cyber-attacks. Planning focuses on steps the State must take to minimize the impact of an attack. Post-exercise lessons learned will be acted on and tracked, improving the resiliency of our critical infrastructure.

Critical infrastructure resiliency has become a national priority in the wake of the Colonial Pipeline ransomware attack in 2021. The best way to prepare for such attacks is through simulated tabletop exercises and assessments that can reveal weaknesses and shortcomings in cyber defenses.

Actions:

- **Increase focus on cybersecurity risks against critical infrastructure.** The State of Connecticut was one of four states selected to take part in GridEx in 2021. GridEx is a distributed simulation exercise led by the North American Electric Reliability Corporation (NERC) and the Electricity Information Sharing and Analysis Center. GridEx simulates a cyber and physical attack on the North American electricity grid and other critical infrastructure. This simulated exercise will help the State better understand threats and responses to those threats pertaining to critical energy infrastructure. The output of GridEx results are still under review and will help inform risk decisions against the electric grid.

- **Conduct cyber readiness activities and risk assessments.** The DAS/BITS security organization will perform annual risk assessment activities, including ransomware preparedness and other cyber-attacks. The output of these assessments will help focus cyber defenses where they are needed most. It is not practical or sustainable to prevent every possible cyber-attack. Therefore, state cyber protection activities will factor in risk assessment that identify risk, likelihood and impact should an event occur. Resiliency planning will take place with other areas of technology, including Business Continuity planning and Disaster Recovery. Partnering across all areas of technology and the agencies will be essential to meeting this objective.

- **Participate in regional cybersecurity preparedness activities.** Cyber Yankee is a regional cybersecurity exercise sponsored by the regional National Guard and designed to promote interoperability of National Guard cyber operators among the New England states and build readiness to respond to network attacks. The State will participate in the 2022 Cyber Yankee exercise, which is being hosted in the State of Connecticut.

As state government develops and implements a strategy to protect their IT assets and data from cybersecurity threats and other disasters, they must also focus on making these services resilient. Ensuring that State networks can adapt, recover, and continue to operate when an attack happens. Embracing cyber resilience planning ensures a method to build comprehensive, long-term strategies on the path toward digital transformation. Resiliency planning will promote a culture of innovation, generate new avenues for investment, and contribute to a vibrant and economically competitive state.

Summary

Strong cybersecurity policy, procedures and controls are critical for our economic development. As government processes and systems are increasingly digitized, cybersecurity will continue to be an important enabler that allows the transition to Digital Government to be safer and more resilient for all citizens.

Cybersecurity risks remain in constant flux. We will update The State Cybersecurity Strategy to respond with these changing threats. The State CISO will review the Strategy annually to ensure that it is current and relevant to the threats posed to state government and to the citizens of Connecticut. The State CISO will ensure that changes to the Strategy are updated and communicated to relevant stakeholders.

Cybersecurity remains a top concern for The State. No single action will protect from growing cyber threats. It will take a coordinated effort from both the public and private sector to ensure the safeness and soundness of our IT systems and citizen data. Trust and security are at the heart of the relationship between businesses, residents, and their digital government. We are delivering on Governor Lamont’s vision of an all-digital government by raising our skills and deploying technology in ways that build confidence of the people we serve.

Resources

Cybersecurity is a continuously evolving topic with both threats and defenses changing daily. Stay informed about the latest cybersecurity threats, learn how to protect your personal and business data, and find solutions for dealing with cyberattacks using the resources below.

Reporting Cybersecurity Breaches in the State of Connecticut

Pursuant to Connecticut General Statutes § 36a-701b, any person who owns, licenses or maintains computerized data that includes personal information is required to disclose a security breach to state residents whose personal information is believed to have been compromised. Note that "any person" includes companies.

Incidents should be reported at the Office of the Attorney General
https://portal.ct.gov/AG/General/Report-a-Breach-of-Security-Involving-Computerized-Data

In addition to the Office of the Attorney General, cases that involve financial loss including ransomware can be reported to the FBI, who have specialized teams set up to help recover funds for victims. You can report suspicious activities and crime by contacting the FBI New Haven office 24 hours a day, seven days a week. You can report cyber incidents using the FBI's Internet Crime Complaint Center (https://www.ic3.gov).

Links to important cybersecurity information.

f

The Center for Internet Security
https://www.cisecurity.org

Connecticut Business & Industry Association Cybersecurity Resources
https://www.cbia.com/resource/category/small-business/cybersecurity/

Connecticut Intelligence Center (CTIC)
https://portal.ct.gov/DEMHS/Homeland-Security/Intelligence-and-Counter-Terrorism

Cyber Incident Reporting Guide
https://portal.ct.gov/cyberreportingguide

Cybersecurity and Infrastructure Security Agency (CISA)
https://www.cisa.gov

Department of Homeland Security
https://www.dhs.gov

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
https://www.cisecurity.org/ei-isac/

FBI Cyber Crime
https://www.fbi.gov/investigate/cyber

FBI New Haven
https://www.fbi.gov/contact-us/field-offices/newhaven

Multi-State Information Sharing & Analysis Center (MS-ISAC)
https://www.cisecurity.org/ms-isac/

State of Connecticut Cybersecurity Resource Page
https://portal.ct.gov/connecticut-cybersecurity-resource-page