JOSH GREEN, M.D.
GOVERNOR

DOUGLAS MURDOCK
CHIEF INFORMATION OFFICER

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES
P.O. BOX 119, HONOLULU, HI 96810-0119

January 8, 2024

The Honorable Ronald D. Kouchi
President of the Senate
and Members of the Senate
Hawai'i State Legislature
State Capitol, Room 409
Honolulu, Hawai'i 96813

The Honorable Scott K. Saiki
Speaker and Members of the
House of Representatives
Hawai'i State Legislature
State Capitol, Room 431
Honolulu, Hawai'i 96813

Dear President Kouchi, Speaker Saiki, and Members of the Legislature:

For your information and consideration, I am transmitting a copy of the report on the State Executive Branch Cybersecurity Program pursuant to SR 75, SD1 (SLH 2023).

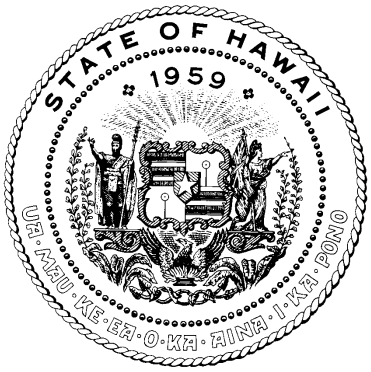
In accordance with Section 93-16, Hawaii Revised Statutes, this report will be posted on the Office of Technology Services website at http://ets.hawaii.gov (see "Reports").

Sincerely,

Douglas Murdock (Jan 8, 2024 12:19 HST)

Douglas Murdock
Chief Information Officer

Attachment



OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

REPORT ON

STATE EXECUTIVE BRANCH CYBERSECURITY PROGRAM

DECEMBER 2023

SUBMITTED TO

THE THIRTY-SECOND STATE LEGISLATURE

CONTENTS

Office of Enterprise Technology Services

State of Hawai‘i

The State Office of Enterprise Technology Services (ETS) submits the following report, pursuant to SR75 SD1, Session Laws of Hawai‘i (SLH) 2023:

> *“Senate Resolution Requesting that the Chief Information Officer ensure that all state departments, agencies, and offices of the state have up-to-date technology to reduce cyber threats and help protect the state against cyberattacks.”*

BACKGROUND

“Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. Defending against these attacks is essential to maintaining the nation’s security. Protecting cyber space is the responsibility of individuals, families, small and large businesses, SLTT and federal governments. By preventing attacks or mitigating the spread of an attack as quickly as possible, cyber threat actors lose their power. Any cyber-attack, no matter how small, is a threat to our national security and must be identified, managed, and shut down. *–Cybersecurity and Infrastructure Security Agency (CISA)*

“Cyber threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.”

–National Institute of Standards and Technology (NIST)

CYBERSECURITY ROLE:
OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

Under Hawai‘i Revised Statutes (HRS) Chapters 26-6(b)(9), 27-43, and 27-43.5, the Chief Information Officer (CIO) and the Office of Enterprise Technology Services, have responsibility to provide centralized cybersecurity for State Executive Branch technology systems. Accompanying statutorily mandated information technology (IT) governance, management, and operational responsibilities collectively support the execution of an effective overall cybersecurity program. Those statutes are listed below.

Summary	Statutory Reference
Provide centralized computer information management and processing services.	HRS Chapter 26.6(b)(9)
Coordinate each executive branch department and agency's information technology budget request, forecast, and procurement purchase to ensure compliance with the department or agency's strategic plan and road map and with ETS' IT governance processes and enterprise architecture policies and standards, including policies and standards for systems, services, hardware, software, and security management.	HRS Chapter 27-43
Provide periodic security reviews of all executive branch departments and agencies regarding the protection of government information and data communication infrastructure.	HRS Chapter 27-43.5
Set policies, procedures, and standards for each executive branch department's reasonable efforts to make appropriate and existing electronic data sets maintained by the department electronically available to the public through the State's open data portal at data.hawaii.gov or successor website.	HRS Chapter 27-44
Provide services through centralized web portal and Internet presence (hawaii.gov) that allow citizens to (securely) conduct business electronically with the government, in accordance with statute (i.e., Access Hawai‘i Committee).	HRS Chapter 27G
Provide guidance to protect personal information that is collected and maintained by State and county government agencies, including best practices to improve security and privacy programs (i.e., Information Privacy and Security Committee).	HRS chapter 487N

STATE CYBERSECURITY PROGRAM OVERVIEW

Strategy. Extend the statewide cyber security strategy to protect the State's IT infrastructure and constituent data through adoption of cyber security industry best practices across the State's IT systems.
Mission: Protect and safeguard data passing through and stored on state government technology infrastructure.

MULTI-TIERED, LAYERED CYBERSECURITY APPROACH

The ETS' "layered approach" to cybersecurity includes adopting secure network topology, technology, hardware, and software tools, continuously monitoring, and sharing information about network and endpoint activities, responding to threats alerts and incidents, and promoting cybersecurity awareness and end user training and education. Together these activities provide flexibility and capabilities to address constantly changing threats and vulnerabilities, to adapt to different risk tolerances, and to apply various preventive solutions, corrective actions, and countermeasures, as appropriate.

ETS CYBSERSECURITY TEAM

The ETS Cybersecurity Team of 15 positions, led by the Chief Information Security Officer (CISO) [who reports to the Chief Information Officer (CIO)] carries out the statewide cybersecurity strategy to protect the State's IT infrastructure and data through adoption of cyber security industry best practices across the State's departmental IT systems and networks.

In addition, about 20 other ETS positions perform some security-related functions part of the time when working with cloud computing services, enterprise software platforms, and data communication networks.

The ETS Cybersecurity Team provides cybersecurity best practices, guidelines, and alerts for executive branch departments to proactively identify and address hardware and software vulnerabilities on devices that connect with on-premise and remote cloud systems and with the State's Next Generation Network (NGN) that ALL branches of State government connect with to access the public Internet where many cyber threats originate.

Through a centralized virtual Security Operations Center (SOC), the ETS Security Team, with external government and commercial support, monitors the statewide enterprise networks, cloud computing systems, and end user devices on a 24/7/365 basis.

For the 12 months of 2023, the ETS SOC reported these experiences:

- detected **eight (8) billion** cyber intrusion attempts
- evaluated **one (1) million** security alerts
- resolved (successfully) **147** cyber incidents

Federal Security Partners. The ETS Cybersecurity Team works closely with the following external service providers:

The Center for Internet Security (CIS)
Multi-State Information Sharing and Analysis Center (MS-ISAC)

To supplement internal staff resources, ETS continued to use a variety of monitoring and assessment services from The Center for Internet Security (CIS), Multi-State Information Sharing and Analysis Center (MS-ISAC), which the U.S. Department of Homeland Security (DHS) has designated as the coordinating entity for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments.

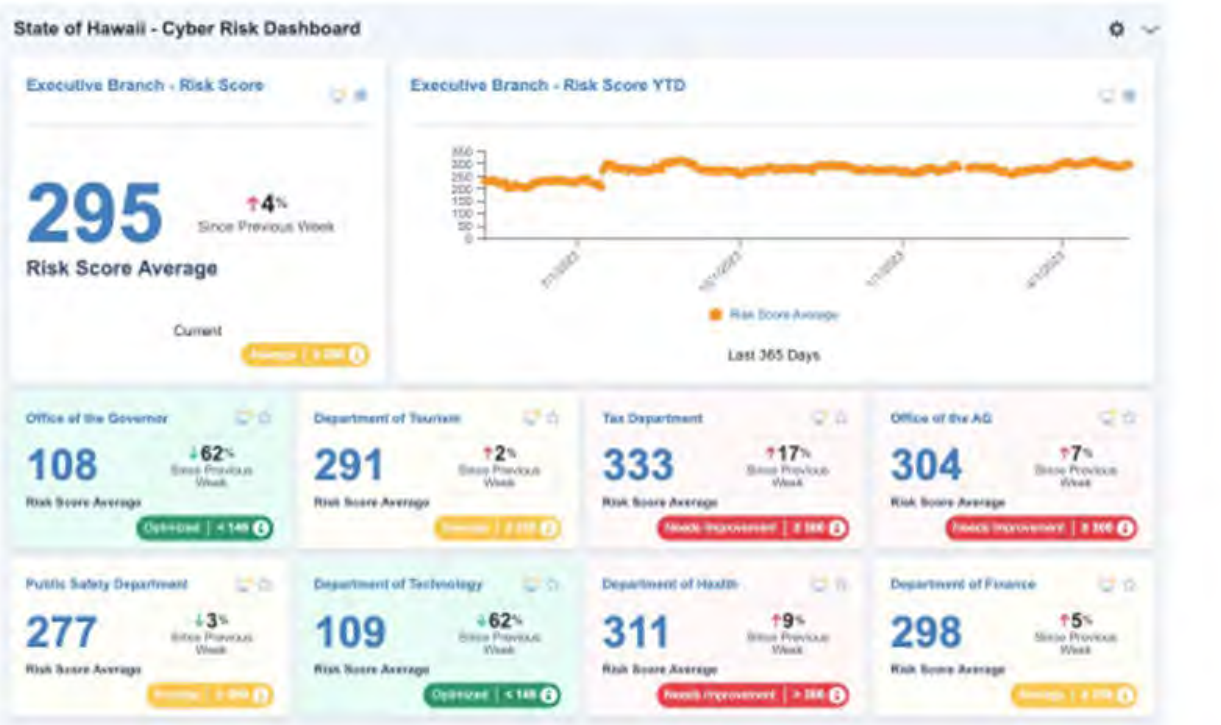
The MS-ISAC's 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response for the broader U.S. SLTT community, with specific tailored services and information to the State of Hawai'i.

For a broader situational awareness of national and international cyber threats and incidents, the MS-ISAC staff are part of the Federal government, intelligence community, and law enforcement team at the DHS' National Cybersecurity and Communications Integration Center (NCCIC), a 24x7x365 cyber situational awareness, incident response, and management center.

Federally funded NetFlow Monitoring and Analysis from CIS/MS-ISAC is an automated process of collecting, correlating, and analyzing computer security information from thousands of networks, desktops, and servers across all State governments. This national Cyber Threat Intelligence (CTI) services available to the States includes security event analysis, notifications, and tailored threat intelligence and remediation guidance that identify attack indicators, mitigate identified threats, establish threat data feeds, and share alerts and advisories of emerging trends and activity patterns across the states, regions, and nation.

Federal Cyber Hygiene Scans. As part of the Federal Cyber Hygiene (CyHy) program, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Protection Agency (CISA) and the FBI regularly scan state department and agency public facing systems to identify vulnerabilities and assess the cybersecurity risks to assist ETS and departments in their corrective actions.

CYBER RISK SCORING PROGRAM



Hawai‘i’s Cyber Risk Scoring Program (CRSP) is based on a risk-based approach to cyber security, using a scoring system to assess the risk of each department information system to cyberattacks such as the following factors:

- Likelihood of a cyber-attack (vulnerability)
- Impact of a cyber attack
- Value of the information system
- Sensitivity of the information system

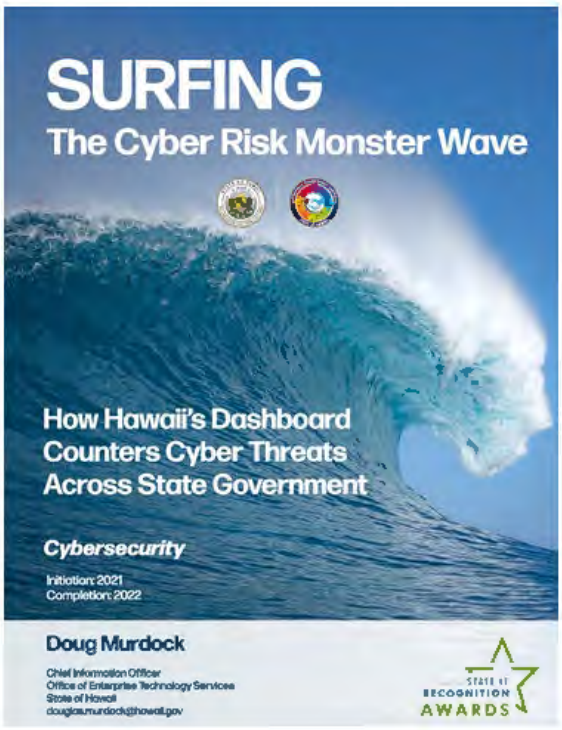
With this scoring information, departments can prioritize resources and investments to mitigate the highest risks and vulnerabilities first, such as old technology, systems that require patches, and those requiring modernization and upgrades.

The Cyber Risk Scoring Program has been a tremendous success to monitor and assess technology assets, improve cyber security posture, and protect the state's information systems from cyber threats before they become costly problems. With this information, ETS regularly notifies departments/agencies of various vulnerabilities and recommendations for remedial action found in a variety of applications, software, and devices.

This tool aggregates risk data from every endpoint in the executive branch into an easily digestible risk score that is updated for state technology managers and state leadership, including the Office of the Governor, State CIO, and State CISO as frequently as every two minutes.

"The Cyber Risk Scoring Program is a continuous improvement process," said Vincent Hoang, Hawai'i's Chief Information Security Officer. The CRSP is constantly being updated to reflect changes in cyber security threats and risks. The program is also designed to be collaborative where ETS works closely with other state agencies and stakeholders to manage their cyber security risks."

The CRSP is built on the Tanium platform which the State of Hawai'i uses to manage and secure state-wide computer systems. The partnership between ETS and Tanium reflects the shared commitment to securing the State of Hawai'i's endpoints so that government data is protected and essential services remain open. Tanium Technical Account Managers meet weekly with the ETS staff to create data-driven and innovative solutions around cybersecurity that save staff time and create higher value for State IT hygiene and cybersecurity management.



STATE OF HAWAI'I'S CYBERSECURITY PROGRAM EARNS NATIONAL RECOGNITION IN 2023

Surfing the Cyber Risk Monster Wave

The National Association of State Chief Information Officers (NASCIO) presented its top cybersecurity category award to the Office of Enterprise Technology Services at its 2023 State IT Recognition Awards Oct. 11 in Minneapolis, MN, for its program: "State of Hawai'i: Surfing the Cyber Risk Monster Wave."

Hawai'i Chief Information Officer Doug Murdock said state governments face an ever-increasing "wave" of cyber threats that, if unmanaged, can lead to devastating consequences.

"To help protect Hawai'i, we developed the State of Hawai'i Cyber Risk Scoring System to deliver real-time visibility around cybersecurity controls and risk posture across all state departments in the executive branch," Murdock said.

SELECTED CYBERSECURITY PROTECTION INITIATIVES

Continuous Internal and External Vulnerability Assessments. ETS has developed an internal vulnerability management platform, that supplements federal vulnerability scanning programs, where ETS and departments can conduct their own vulnerability assessments of their assets and work with ETS to address needed fixes, updates, investments, and training. ETS continues to improve the effectiveness of regular internal and external scans to identify vulnerable devices.

Protecting Critical Infrastructure. ETS also works to enhance the cybersecurity of critical infrastructure providers and continues to improve coordination of county, city, state, and federal government activities that provide security online and fight cybercrime. As one example, ETS provides the virtual computing, communication network infrastructure, and many layers of cybersecurity protections for the statewide state-city-county elections systems which the Department of Homeland Security has designated as a critical infrastructure. And another example, ETS and the State Office of Homeland Security jointly developed, updated, and exercised the State's Cyber Incident and Cyber Disruption Response Plans, that strengthened response coordination between state and local agencies.

Local Enterprise Security Information and Event Management. The Security Information and Event Management (SIEM) system collects and analyzes thousands of security events and logs from internal monitoring points. Alerts, notices, and suggested actions are transmitted to departments for their awareness and remedial action.

Endpoint Security. ETS and state departments have deployed anti-virus and anti-malware and end point security agents to over 18,000 individual computing devices to reduce risks of cyber attacks and loss of data. This especially minimizes risks for outdated devices and older technologies that may be more vulnerable. These smart remote agents and management tools permit ETS and the departments to quickly detect and respond to evolving cybersecurity related threats.

Security and Protection Benefits of Microsoft Office 365. With all state executive branch departments* using the Microsoft Office 365 platform, the full range of Microsoft protection and security tools are available, including:

- Data loss prevention (DLP) protects against data leakage, e.g., Social Security numbers and other personally identifiable information (PII).
- Security and management software tools providing improved activity monitoring, patching, and access controls.
- Enhanced, easy-to-enable email encryption, e.g., by simply typing *secure* in the subject line.
- Microsoft Intune and endpoint protection for departments to better manage their endpoint devices.
- Built-in mobile device security via Microsoft Enterprise Mobility.

**(Department of Education and University* of *Hawai'i adopted Google Gmail education platform).*

Mandatory Multi-Factor Authentication (MFA). As part of the Microsoft Office 365 roll-out, MFA is required for all accounts to enable strong identity and access management (IAM) policies. As an authentication method, MFA requires user to provide two or more verification factors to access an application, device, or online account. In addition to requesting a username and password, MFA requires one or more additional verification element, such as text message to phone, fingerprint, or uniquely generated code to reduce the likelihood of a successful account access if a password is compromised, i.e., someone with your account name and password requires another piece of information to access the account or device.

External email label. This added email descriptor makes external e-mail easy to identify while making internal e-mail more difficult to impersonate to reduce the risk of phishing. Over a 12-month period, this email tagging security solution detected over 50,000 malicious emails, blocking 98%.

Robust email spam filtering. A new email filtering system classifies email as spam or junk, creates a spam email digest, and sends it to a personal quarantine outside the email system, instead of delivering to the inbox or junk folder.

Web security and performance enhancer. This provides cyber-attack mitigation through web application firewalls that increase website security and improve performance, content delivery, and network services.

Government domain names @Hawaii.gov. ETS worked with state department public information officers to adopt and use the **@Hawaii.gov** address for all e-mail and web names to gain the added benefits, protections, and security afforded to **.gov** government domains.

Hawai‘i Citizen Single Sign-on. Over 70 online portal services now use the eHawaii.gov Single Sign-On (SSO) service where citizens use one secure credential to log-on to many public-facing websites that provide government services. ETS is expanding this secure Microsoft Entra External ID and Azure AD B2C solution to other state online services/portals.

Dynamics Fraud Protection. ETS worked with the Department of Human Services (DHS) to architect and implement Dynamics Fraud Protection to provide more robust end-user authentication security and identity proofing for Business-to-Consumer (B2C) access to public-facing government applications.

ENTERPRISE CYBERSECURITY GOVERNANCE

IT Budget Reviews. HRS section 27-43, authorizes the CIO to coordinate each executive branch department and agency's IT budget request to ensure compliance with ETS' IT governance processes and enterprise architecture policies and standards, including "*policies and standards for systems, services, hardware, software, and* ***security management***."

As part of this enhanced IT governance authority, ETS works closely with the Department of Budget and Finance (B&F) to review IT-related funding requests, such as for security programs, in the annual budget request process, as directed by Executive Memorandum Budget Execution Policies and Instructions.

ETS' IT Governance implements and coordinates the governance process required by the Administrative Directive No. 18-03 – Program Governance and IV&V Requirements for Enterprise IT Projects. The state's IT project portfolio governance consists of project phase review gates to ensure project execution and associated expenditures are sufficiently evaluated and receive approval by the appropriate state governing bodies.

ETS reviews and evaluates departmental IT budget submittals against established criteria, and provides input and feedback to B&F on those IT requests. ETS follows a contract management process, where draft requests for proposals and draft vendor contracts for enterprise IT projects and initiatives are reviewed for best practices. This review integrates this new information into the State's overall IT strategic plans and roadmaps.

Quarterly Cyber Security Reviews. To augment the annual IT budget reviews, ETS has quarterly security reviews with departments to focus resources on higher priority and identified critical security and vulnerability initiatives that require addressing.

CYBERSECURITY AWARENESS AND EDUCATION: CRITICAL ELEMENTS

Continuous cybersecurity training and education is critical to the overall cybersecurity program since uninformed, mistaken, and erroneous user behavior can comprise even the most secure computing environment. Recognizing that improving cybersecurity preparedness is a shared responsibility among many, ETS conducts various cybersecurity awareness and education activities that focus on cyber threat prevention and protection best practices to increase the understanding of cyber threats.

As one example, ETS has been working with the State Department of Human Resources to provide Cybersecurity Awareness Training as part of the State's foundational knowledge set for all employees. And ETS is working with departmental IT staff on a variety of exercises to improve cybersecurity skillsets and capabilities of State IT teams.

Cybersecurity Month. Governor Josh Green, MD, proclaimed October 2023 as Cyber Security Awareness Month in Hawai'i, in recognition of the state's role in identifying, protecting its citizens from, and responding to cyber threats.

"This year marks the 20th year of Cybersecurity Awareness Month, which helps to raise awareness about cyber risks and encourages everyone to engage in safe online practices to protect themselves from malicious cyber actors," said Governor Green. "Every year cybersecurity becomes more important as our daily lives depend more and more on safe online communications."

The proclamation supports the state's continuing work on several cybersecurity initiatives, such as promoting educational opportunities like CyberStart America and developing a skilled cyber workforce by working with the lower and higher education communities.

"Cybersecurity is critical for the state as threats continue to increase around the world. We are constantly working to improve and strengthen our cybersecurity strategies. Being vigilant about personal cybersecurity is key to protecting your finances and keeping your family secure," said State Chief Information Security Officer Vincent Hoang of the Office of Enterprise Technology Services.

During Cybersecurity Awareness Month, ETS and the MS-ISAC offers the "Cybersecurity Toolkit" designed to help end users make proactive positive and effective cybersecurity behavior changes to improve their cybersecurity. The State Department of Commerce and Consumer Affairs, Office of Consumer Protection, also works to identify potential personal cybersecurity attacks to protect our residents from fraudulent online activities (). The State Department of Defense, Office of Homeland Security provides planning and training efforts to prevent, protect, mitigate and respond to government cyber threats.

Cybersecurity Exercises

ETS coordinated enterprise-wide tabletop exercises with department IT staff to practice the high level communication, coordination, and procedural tasks required to effectively respond to cyber incidents.

Phishing Exercises

As phishing emails and related social engineering campaigns are today's number one attack vector that injects malware, ransomware, trojans, spyware, viruses, worms, keyloggers, bots, and other types of malicious software.

ETS conducts cyber security awareness campaigns quarterly through simulated phishing emails to educate and empower all employees (not only IT staff) to be safe and secure when using computing devices, and provides access to resources, tools, and training they need to make more informed decisions when on-line using the Internet.

When employees click on a "suspicious" link or attachment in a simulated phishing email, the resulting message explains that they have potentially put both themselves and the organization at risk. That screen and subsequent screens are "training pages" explaining why phishing is harmful, reinforces the dangers of phishing, and reminds employees how to detect and report suspected emails.

In a recent phishing campaign, a "suspicious" message was delivered to 12,912 mailboxes; 978 (7.6%) users "clicked on" a link in the "suspicious" e-mail. During the campaign, 228 (9.8%) users reported that "suspicious" e-mail to ETS, with the first user submitting a "suspicious" email report within 1 minute after the phishing email was sent.

FUTURE ETS CYBERSECURITY INITIATIVES

Building upon the strong foundation of current security tools, policies, and methodologies, ETS' cybersecurity priorities and next steps to effectively meet challenges of the constantly changing cyber threat landscape and cyberattack methods, includes four general areas described below to be implemented when resources permit:

Investing in Employees. Providing expanded eEducation and training will significantly increase department IT staff cybersecurity skills and capabilities through exercises and professional development.

Extending Internal State Security Operations to 24/7/365. Adding these staffing hours and availability will provide more timely local incident response, build internal proactive investigation capabilities to identify new threats and Internet-facing vulnerabilities, conduct expanded vulnerability assessments and penetration testing of internal networks, and further expand department endpoint device and patch management. While the mainland-based MS-ISAC provides nominal 24/7 monitoring, there is no local staff available to immediately respond during outside normal business hours.

Investing in the critical state communications network. As network connectivity and Internet access is essential today, updating the statewide data communications infrastructure will be critical to maintain secure connectivity for daily tasks, and more importantly, for emergency and disaster response, e.g., after recent Maui wildfires destroyed the entire commercial communication infrastructure in West Maui, only the State's first responder communication assets continued to function during and after the disaster. Planning to replace many key communications and security components that are approaching end-of-life is a high priority to continue secure and continuous government communications.

Evaluate and adopt artificial intelligence (AI) components. As adversaries and cybercriminals use AI to undertake a variety of sophisticated attacks, adding AI to the cyber defense arsenal will be essential to quickly detect suspicious activities or block AI-based attacks, and to rapidly identify weaknesses before hackers can maliciously exploit them.

This report does not include specific threats, vulnerabilities, countermeasures, or sensitive information that could compromise our overall cybersecurity. The ETS Security Team is available to the Legislature, upon request, to provide a more comprehensive briefing with additional details in a secure environment.