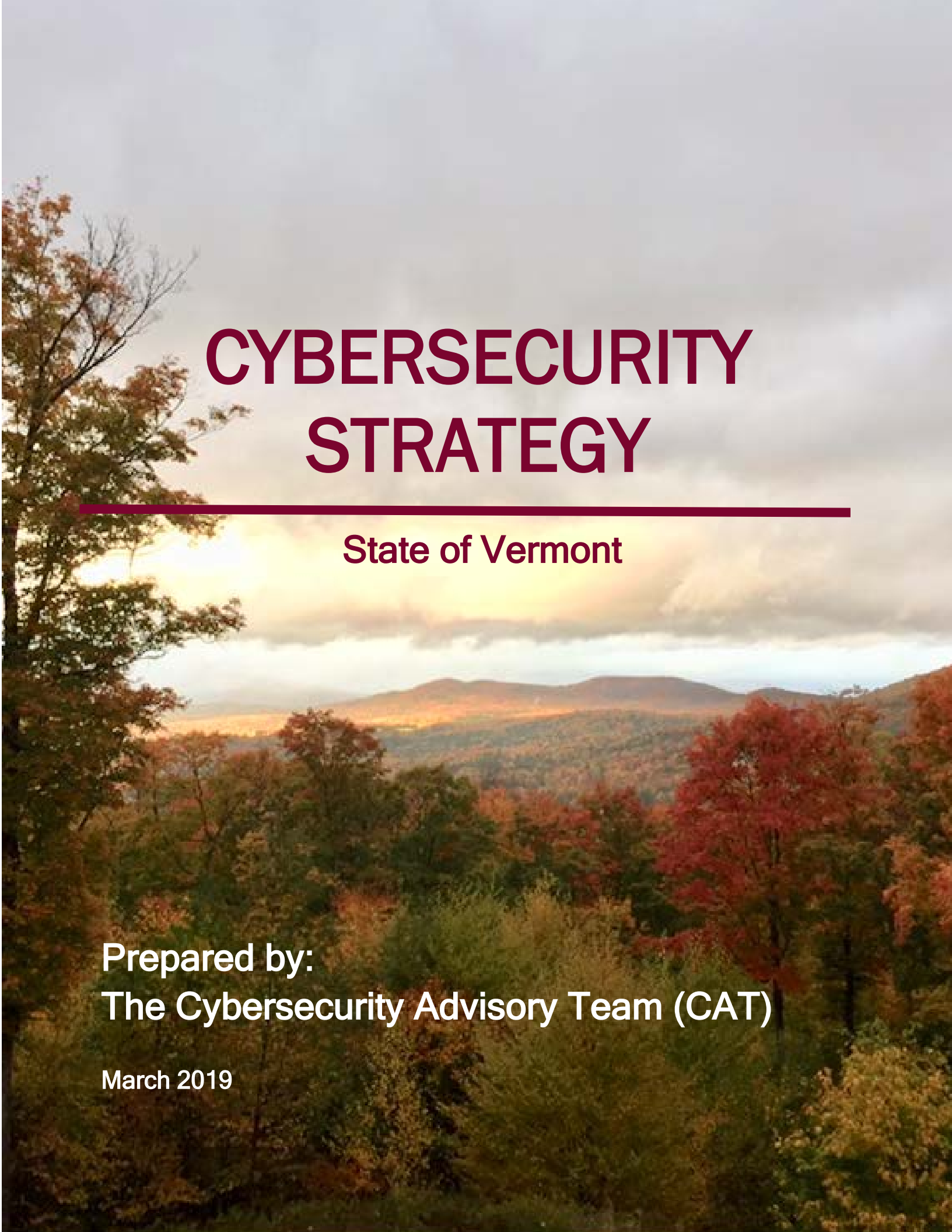


CYBERSECURITY STRATEGY

State of Vermont

Prepared by:
The Cybersecurity Advisory Team (CAT)

March 2019

Message from the Governor

Technology has become a necessity for business and government. That is why I created the Cybersecurity Advisory Team and tasked them with developing a cybersecurity strategy. This work is a critical component of meeting the strategic goals of my Administration.

- **Growing the Economy**: With increased cybersecurity awareness, education and capacity, our businesses can continue to grow and thrive. Tackling these challenges provides us with an opportunity to expand Vermont's workforce with next-generation skillsets that will create an in-demand population of workers across agencies, sectors, and industries to strengthen our economy.

- **Making Vermont More Affordable**: We will use this strategy as our roadmap to bolster cybersecurity in support of modernizing state government. Through public-private partnerships, we will not only create new job opportunities in Vermont but will also protect the investments made in our critical assets, infrastructure, services, and personal information - driving down cost through greater collaboration, information sharing, and preparation.

- **Protecting the Most Vulnerable:** In partnership with federal, state, and local governments, private businesses, non-governmental entities, and academic institutions we will promote awareness of the threat that cybersecurity risks pose to our families and way of life. We must protect our state's most vulnerable citizens – a responsibility that extends into cyberspace and the unique challenges we face.

We must all be proactive, embrace the digital age, and make cybersecurity a part of our everyday lives.

I want to thank my Cybersecurity Advisory Team for their hard work and dedication in putting together a strategy that will guide us in protecting valuable assets.

Philip B. Scott
Governor

I. Executive Summary

The Cybersecurity Advisory Team (CAT) is charged by Executive Order 18-17 to develop a strategic plan, evaluate statewide cybersecurity readiness, build relationships and lines of communication, and build strong partnerships that help protect the data, information systems, and privacy of State government, Vermont businesses, and the public. The CAT is additionally charged to identify and advise on opportunities to enhance the workforce, raise citizen awareness, provide training and technical capabilities, provide expertise to assist the State Legislature with statutory language, budgetary impacts, and engaging State and Federal partners as it relates to cybersecurity.

Increasingly sophisticated attacks of advanced complexity attempt to breach and cause damage to systems representing an ongoing threat to the State's economy, critical infrastructure, and privacy. Inaction has a cost that can be measured financially, through loss of confidence our institutions, and by exposing the private information of our citizens. The potential harm must be taken into account, and our constituents must be aware of the threats.

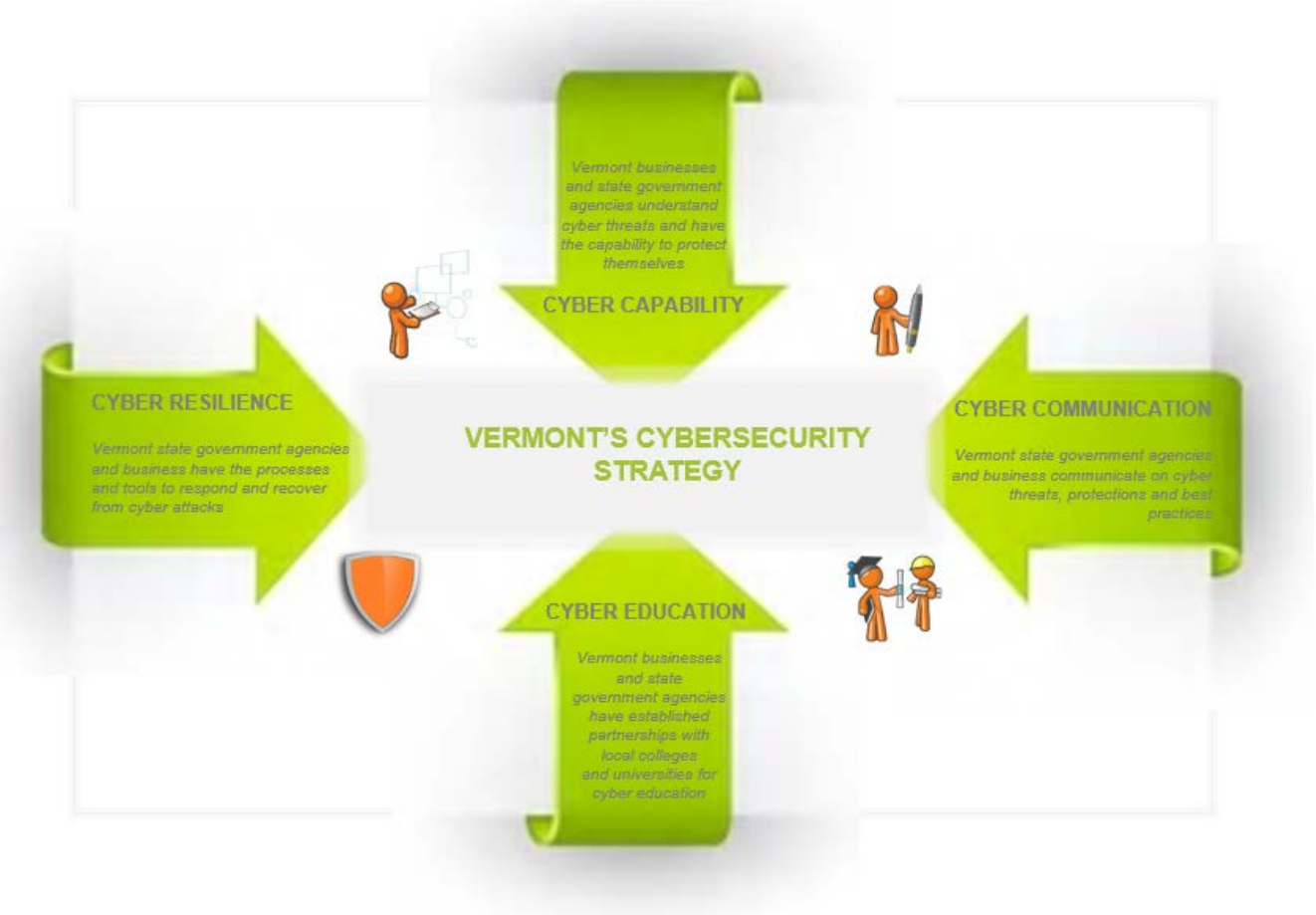
Our State already has kicked-off initiatives to address some of our risk. The implementation of a Security Operations Center (SOC) and updates to the State Emergency Operations Plan are examples of this. The team used the model of the National Institute of Standards and Technologies – Cybersecurity Framework (NIST CSF), a set of guidelines and best practices to reduce cybersecurity-related risk, to facilitate prioritization and ensure alignment with other sectors. The purpose of this document is to assist with the identification and implementation of new initiatives through the following pillars:

- CYBER CAPABILITY (NIST CSF - Protect & Detect) - Improve Vermont's digital security through increased knowledge, enhanced workforce development, and improved technology to protect and defend against, as well as reduce the risk of, future cyber-attacks.

- CYBER RESILIENCE (NIST CSF - Respond & Recover) - Increase Vermont's ability to respond to and recover from cyber incidents. Decrease potential disruption, financial impact, intellectual property loss, and violation of privacy.

- CYBER COMMUNICATION (NIST CSF - Identify) - Expand Vermont's communication, coordination, and awareness between entities such as state and local government agencies, businesses, and citizens to improve understanding of risk.

  CYBER EDUCATION - (NIST CSF – Protect) Build strong partnerships with local universities and colleges to enhance cyber education of Vermonters enabling the improvement of cyber capability, the expansion cyber communication, and the increased cyber resilience.



II. Introduction

STATEMENT OF INTENT

To achieve success with this strategy, the CAT has assigned roles and responsibilities to the stakeholders affected by this initiative and outlined next steps to take toward implementation. Participants ranging from State government to the business community to the citizens of Vermont must all do their part to bring about the goals above. Effective coordination and a team effort is required to meet the listed objectives. Follow-through is necessary to take the strategic principles from this document and create operational plans that support this strategy. Identifying gaps, assessing risks, and determining the resources to accomplish the principles some of which may be realized in the short-term or some may take years to achieve.

The means of potential attack vary from phishing attempts to implanting malicious malware in individual or networked computer systems. This can impact individual homes, corporate business systems, government agencies, or critical infrastructure that sustains life and provides for the essential functions of government. Larger scale regional or national attacks could shut down essential services, the impact of which could be catastrophic to all who live, work, or play in Vermont. The consequences of unchecked cyber dangers are diverse and serious, and they represent a threat to the daily life of all Vermonters.

Though the majority of security breaches result from external actors, a significant percentage are caused by insiders that may manifest as user error, poor security practices, or intentional harm. These can include accidentally published information, lost backup tapes or laptops, or failure to secure devices in the possession of ex-employees. Some result in theft or destruction of data. Many security issues that impact the citizenry can be avoided through basic security hygiene, education, and security controls.

COST OF INACTION

The severity of potential harm and the fact that no one is immune must be heard loud and clear. Those involved in protecting the security and well-being of our state must act. The public and private sectors must commit fully to the growing cyber threat reality. Strategies and action plans need to be developed by the state, individual agencies and private entities. The Cybersecurity Strategy for the State of Vermont must deliver effective capabilities and outcomes that will allow Vermonters to realize the benefits and competitive power that will come from living in a safer, more cyber-aware state.

HISTORY OF CYBER INCIDENTS IN VERMONT

The following are recent high profile cyber incidents that occurred in Vermont over the past several years:

In June 2017 two of Vermont's biggest businesses, the University of Vermont Medical Center (UVM) and Global Foundries, were significantly affected by phishing attacks. Hackers attempted to break into these business information systems.

At UVM Medical Center, the email accounts of two employees were accessed by third parties after the employees accidentally opened phishing messages that mimicked an official company communication. This was the first time the email system was penetrated in this way despite thousands of prior daily phishing attempts.

An attack using a virus at Global Foundries infected a number of manufacturing tools at the microchip facility in Essex Junction, and some tools were taken offline to isolate the attack and prevent the virus from spreading.

In March 2017 the Vermont Department of Labor reported a data breach on the standalone, web-based database, America's Joblink Alliance (AJLA) that is shared by ten states, including Vermont. A system modification implemented in October 2016 created a vulnerability in the

system. The breach compromised as many as 182,000 accounts in Vermont and 4.8 million accounts across ten states. The breach potentially exposed personal information, including name, date of birth and social security number. For Vermont, these are accounts entered into Vermont Joblink over a 14-year period. Some users voluntarily register, and others are required by VDOL to register for the program.

A March 2017 a Vermont Digger article reported that Vermont is a consistent target for cyber-attacks and in the first two months of 2017 the Vermont state government faced:

- 65,000 malware phishing attacks
- 90,000 remote scans – attempts to identity targets for attack
- 575,000 other "digital bombardments."

In December 2016 it was reported by the Washington Post that hackers affiliated with the Russian government had penetrated the United States electric grid by attacking the Burlington Electric Company in Vermont. The story was originally illustrated with an image of the headquarters of a Russian spy agency, which it alleged was behind the intrusion. Months later, FBI investigators reported that the attack was not validated and that the internet traffic that raised the red flag may, in fact, have been harmless.

The Vermont Intelligence Center, whose goal is to identify patterns and indicators of cybercriminal and terrorism-related activity in the State of Vermont, has tracked thousands of cyber-attack incidents in Vermont and during 2017 recorded the following breakdown:

- 58% - Ransomware & malware attacks (Botnet attacks)
- 27% - Computer compromises or network penetrations
- 13% - Data Breaches
- 2% - Web defacements

CURRENT STATE

Most cyber incidents are unreported or are undiscovered. A February 2018 article by the New York Times headline reads: “An ‘Iceberg’ of Unseen Crimes: Many Cyber Offenses Go Unreported”. This article summarizes its findings with the following: “In a sense, technology has created an extraordinary moment for industrious criminals, increasing profits without the risk of street violence. Digital villainy can be launched from faraway states, or countries, eliminating physical threats the police traditionally confront. Cyber perpetrators remain unknown. Law enforcement officials, meanwhile, ask themselves: Who owns their crimes? Who must investigate them? What are the specific violations? Who are the victims? How can we prevent it?

III. Strategy

SCOPE OF STRATEGY

The Cybersecurity Advisory Team has developed a strategy document that encompasses all Vermonters who live, work, and play in the state. This work includes education, research and best practices developed and implemented in other states, the federal government and other countries. Vermont agencies have participated in multiple working groups including the National Governors Association and the Federal Emergency Management Agency (FEMA) Region 1 cyber working group.

The State and local government strategy will be a multi-facetted approach encompassing the following goals.

- The State of Vermont will use an enterprise wide approach to secure and make resilient the State of Vermont’s cyber infrastructure and data.
- The State will deliver an improved response to the growing area of cybercrime and cyber breaches which will include *consequence management.*

- Vermont will leverage and capitalize on the growing cybersecurity job market through education, workforce development, and economic development.
- Vermont will focus on education and outreach to all sectors, including the public, to create a more resilient Vermont.
- Local government will be incorporated into this strategy recognizing that most resources at a local level are extremely limited.

The State of Vermont will achieve these strategic goals by prioritizing the accomplishment of the following objectives:

State and Local Government in Vermont:

- Focus State government agencies on cyber prevention, protection, response and recovery.
- Establish a risk management framework to apply resources that are informed by an assessment of cybersecurity vulnerabilities and cybersecurity threats.
- Identify state and local cybersecurity gaps and develop mitigation strategies.
- Support continuing efforts relating to cybercrime interdiction and disruption as it affects Vermont, partnering with local, federal, and other state entities.
- Enhance the State's cyber threat intelligence network to support continued situational awareness and information-sharing for state, local, and private sector stakeholders in Vermont.
- Develop a cyber-awareness campaign to educate state and local government, the private sector businesses, and the citizens of Vermont.
- Build a cybersecurity education pipeline through increasing STEM programs in the K-12 educational system and providing support for K-12 cyber-focused extracurricular activities.
- Establish partnerships with Vermont's higher education community in creating certificate programs for cybersecurity education programs.
- Build marketing and economic development strategies to attract citizens into a cybersecurity workforce in support of Vermont government and industry.

- Develop a business plan for exporting these skills to other jurisdictions through telecommuting opportunities.

In addition to the state and local governments, there are several other groups that this strategy will impact. The state will actively seek their participation in the development of governance and the necessary operational discipline to implement the strategy. To develop a comprehensive "all of Vermont" operational plan, the State of Vermont will work with the following groups. For each of these group, there are a set of specific and relevant objectives.

Critical Infrastructure Stakeholders in Vermont:

- Engage critical infrastructure owners and operators in cybersecurity strategies to enable continuity of operations and resource sharing.
- Foster continuous response and recovery improvement through state, local, and critical infrastructure exercises focusing on cyber incident consequence management capabilities.

Private Sector in Vermont:

- Initiate outreach programs to develop partnerships with Vermont businesses.
- Identify business cybersecurity needs and opportunities to share best practices.
- Coordinate prevention, response planning, information sharing and resiliency initiatives.
- Engage the private sector to develop solutions to risk management resource challenges.
- Develop strategies to increase cybersecurity business opportunities in Vermont.
- Engage private sector partners in continued cybersecurity emergency exercises and improvement planning.

Citizens of Vermont:

- Initiate outreach programs to educate Vermont citizens on cybersecurity protection principles and resiliency, cybersecurity awareness and best practices.

MISSION AND VISION

The first steps of developing a strategy is to define our mission and vision. Our mission defines our purpose and primary goal. The effect of a mission statement is to ensure all parties understand the purpose of the Cybersecurity Strategy for the State of Vermont.

Our vision statement focuses is where we want to be and what we want to become in the future. It is our dream. The ideal end state that captures the goals and aspirations.

MISSION

To Improve Vermont's Cybersecurity.

VISION

A cyber secure and resilient Vermont where it is safe to live, work, and play.

STRATEGY

To achieve our vision, the following strategic principles have been set.

CYBER CAPABILITY (NIST CSF- Protect & Detect)

Improve Vermont's digital security through increased knowledge, enhanced workforce development, and improved technology to reduce the risk of future cyber-attacks.

The pace of development of technology is increasing and access to computing power is transcending our entire society. We engage technology for even the most basic tasks and to make our lives easier, safer, and faster. This rapidly changing environment of technology also makes the cyber-criminal or hacker more effective as they mechanize their tactics and techniques. The omnipresence of technology creates a permanent surveillance culture with less privacy. With all the benefits to our lifestyles that is brought by technology we must remain ever vigilant as it makes us more vulnerable to compromise. As the technology develops, we must continue to focus on the foundational and unique elements of our free and open society as we build the necessary and interrelated frameworks in law, policy, and technology. This requires us to evolve not only the technology but also our understanding of the related benefits and risks of such technology. Risk assessments of any technology must include a predictive analysis that identifies the potential for exploiting the technology itself, or the vulnerabilities of the technology, for malicious intent.

Nationally we are experiencing a severe shortage of cybersecurity professionals at all levels. Existing sources of education and training are not producing the entry-level talent. Job openings require advanced skills and experience. The workforce development gap exists in the cybersecurity field specifically but also in awareness across our enterprises. The reality of our present engagement and use of technology means that we as individuals must remain ever vigilant for ourselves and our institutions. We must strive to be perfect in our defense with the understanding that an attacker only needs one flaw or hole. This requires an awareness of the risks, threats, and vulnerabilities of our technologies for all users. Basic "cyber hygiene" and cyber awareness is required of all citizens.

Response to this crisis will require a portfolio of efforts that include: attracting more college students into this career field; engaging students in our K-12 programs; creating pathways for veterans and mid-career professionals to enter the cybersecurity field; developing and experimenting with innovative programs, internships, and apprenticeships to staff these essential functions; supporting the development and rollout of cyber awareness education at all levels from Pre-K through senior citizen to be safe and aware of online risks. Local Vermont organizations, such as CyberPatriot and GirlsGoCyberStart, have already demonstrated a commitment to building technical skillsets and cyber awareness in the youth of our state. These programs, and others like them, should receive our full support and are to be commended for shaping the next generation of cyber-savvy Vermonters.

We cannot solve the shortfall in workforce and secure our populace with education and training alone. Technology continues its rapid development and at the same time increased malicious and criminal intent flourish. The technology that connects our lives and increases our productivity is used to create a better phishing email or exploit. We must foster the development of secure systems and practice building security into our technology at conception and not bolted on as an afterthought. Inspecting our existing technologies for flaws and keeping our technology current is critical as our adversaries become more sophisticated and prey upon systems that fall behind. In this environment, we should also understand the policies and requirements to attract cybersecurity research and development activity. Building an active capability in cybersecurity research and development within our higher education institutions and supporting partnership with the private sector and federal government is a significant growth opportunity for Vermont.

CYBER RESILIENCE (NIST CSF – Respond & Recover)

Increase Vermont's ability to respond to and recover from cyber incidents. Decrease potential disruption, financial impact, intellectual property loss, and violation of privacy.

Vermonters need to be prepared to identify, respond and recover from cyber threats. If you use technology at home, work or when you engage in some level of play, ask yourself the

following questions: What would you do if all of your computers and smartphones were encrypted by Ransomware? Do you know if your business is currently breached by a criminal hacker? Do you have a plan in place to deal with these issues?

Our societal reliance on technology is a true testament to how important cyber resilience is. Can you go a day or even a week without technology? How about your place of employment? If there is a disruption in a small businesses' network/website, it may cause significant harm to not only productivity but revenue. Criminals are compromising business assets and capitalizing on the sale of information. According to the 2018 Verizon Data Breach Report, 76% of all data breaches were financially motivated. No sector in Vermont is immune to the threat.

We need to decrease the potential for cyber disruption by educating Vermont on good cyber hygiene. What happens if your personal information is leaked online? How about if your most confidential files at work were now public or for sale on the cyber black market? Do you have a plan? Response from these types of attacks requires proper planning so you can quickly recover from the incident. Identifying key personnel and who is accountable for said activities is also critical. The last thing you want is to be in the middle of an incident and trying to answer questions like:
"Who is responsible for securing our most important files?" and
"When was the last time we changed the password to our administrator account?"

Creating a good cybersecurity culture that promotes cyber resilience is key because without it we don't stand a chance against financially motivated attackers. We must start with education of our children in K-12. We must continue ongoing education of our citizens as they enter higher education and the job market. Every sector of the economy must invest in ongoing education of its employees, constituents and customers. Such education must continue to evolve, keeping pace with the ongoing development of new technologies, identification of new vulnerabilities, discovery of new strategies employed by cyber criminals, and emerging trends in cybersecurity.

Proactive cybersecurity monitoring will save money and reputational capital if your organization finds itself the victim of a cyber-incident. According to Forbes, costs averaged $3.86 million per breach in 2018. The costs typically include legal, forensics, breach notification, and fines by regulators if you are found negligent.

Vermont businesses have worked very hard developing their intellectual property. We are very proud to have organizations that hold patents and trade secrets that they use to develop their products and grow their business. For this reason, Cyber Resilience has become a critical business capability that employs cybersecurity controls and procedures to protect intellectual property and sustains a business's ability to operate.

Privacy violations may involve the loss of regulated data, such as health or personally identifiable information. Such information must always be secured. When an organization possesses personally identifiable information, they must understand that they have been entrusted with one of the most precious assets of our citizens – *their personal information*. That position of "trust" requires, and even demands, the implementation of appropriate Cyber Resilience measures. Data, and information created from that data is essentially the life blood of government and business. It must be properly managed and protected. When that data and information constitutes personally identifiable information there is a higher order of responsibility and accountability for protecting it.

CYBER COMMUNICATION (NIST CSF- Identify)

Expand Vermont's communication, coordination, and awareness between entities such as state and local government agencies, businesses, and citizens to improve understanding of risk.

Cybersecurity today is a team sport with private sector, government, and law enforcement sharing information and working together to defend, respond, and recover. Responding to this challenge is the development of Cybersecurity Information Sharing activities. Federal statute creates an environment where diverse institutions can share best practices, understand the threats, and prepare to respond and recover. An Information Sharing and

Analysis Organization, ISAO, should be developed to meet this critical need. Vermont should create an Integrated Public-Private program for information sharing in the state. The ISAO should perform cybersecurity and threat information sharing and analysis engaging the public and private sector organizations to meet the cybersecurity crisis. We must develop a local, state trust-based threat and incident information sharing capabilities that can network nationally and support local businesses and government. The ISAO will build a local constituency that includes partnerships with the private and public sectors. The purpose of this ISAO will be to share alerts and threat information, provide updates regarding the status and severity of any threat, and provide assistance to ISAO members related to response and recovery. Over time as the ISAO matures in terms of governance and operations it will gather, analyze, and disseminate critical infrastructure information, for the expressed purpose of:

- Sharing Cyber Threat Analysis and Information
- Conducting risk-based analysis
- Assisting in access to resources
- Developing incident response guides and playbooks
- Planning and conducting exercises to assess and improve response and recovery
- Sharing best practices
- Developing operational discipline for cyber disruption response planning

This center should build upon resources available nationally from Information Sharing and Analysis Center, such as the Multi State-ISAC (MS-ISAC), the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC), the National Association of State Chief Information Officers (NASCIO), and others. The State activity will offer a more flexible and responsive to local requirements of information sharing activities among private-public across sectors. This activity will foster collaboration and facilitate the development of trust- based relationships which are essential for effective and efficient cybersecurity information sharing and building a more resilient state.

CYBER EDUCATION (NIST CSF – Protect)

Build strong partnerships with local universities and colleges to enhance cyber education of Vermonters enabling the improvement of cyber capability, the expansion of cyber communications, and the increased cyber resilience.

Vermont has a robust higher education sector with significant expertise in computing, technology, and cybersecurity. Higher education institutions are actively engaged in our communities supporting K-12 education, local government and non-profits. We need to fully leverage these partnerships to build the cyber workforce, protect our critical infrastructure, defend our local municipalities, and ultimately create a more resilient Vermont. With imagination and creativity, we will collaborate with higher education to put in place a pipeline of talent to bring college interns and graduates into this mission. The benefits for students and graduates include an entry point into a rewarding career in cybersecurity and an opportunity to gain experience working on real world incidents. The benefits for government and industry include the creation of an ongoing pool of talent that will bring fresh ideas to problem-solving and qualified individuals able to fill the many roles in cybersecurity.

Vermont is in a unique position with two nationally recognized Centers of Academic Excellence in Cyber Defense Education (CAE-CDE), as designated by the Department of Homeland Security and the National Security Agency. Champlain College and Norwich University are leaders in cybersecurity education and actively engage in cybersecurity efforts within the state and beyond. These two schools, working individually and in concert, have developed programs that support law enforcement, small businesses, municipalities, and state government in becoming more secure. Building on these partnerships provides competency-based education opportunities for students, professional development and research for faculty, and qualified cybersecurity services for the communities they engage. Encouraging and enhancing these partnerships will help meet our workforce requirements and entice graduates to stay in Vermont.

IV. Roles and Responsibilities

The organizations listed below have the responsibility to remain active and engaged in implementing this strategy. Effective coordination and a team effort are required to meet the objectives of this plan. Participating organizations have been chosen for their unique roles or expertise in one or more of the strategic objectives.

Cybersecurity Advisory Team - The Cybersecurity Advisory Team will lead the effort to coordinate communications, projects and programs for fulfilling this strategy. At its discretion, the Team may create inter-agency working groups for planning and operations.

State Government - State Government will participate in the efforts of the Cybersecurity Advisory Team by providing personnel and resources to lead and support those efforts. State Government will facilitate initiatives for achieving the desired outcomes of this document, and lead the development of strategic partnerships with Federal, State, Local, and Private organizations. State Government will review project plans and provide feedback regarding timing and staging of projects as well as technical and financial feasibility.

VIC/Fusion Center - The Vermont Intelligence Center (VIC), in conjunction with the Fusion Center, will provide information trending of the cybersecurity threat landscape and advise the Team on capabilities that exist between the State and external agencies and federal partners. VIC and the Fusion Center will engage in contact and consultation with external agencies and federal partners to leverage their capabilities that may support this strategy.

Other State & Local Agencies - Other State Agencies may be called upon when there is a requirement for their subject matter expertise or when the Team believes that direct coordination with one or more agencies will further the goals of this document. Just as with any other significant event that impacts the State, it is also critical that state agencies are in alignment and working together to develop solutions related to cybersecurity. Coordination of state-level response and recovery to all hazards occurs within the Multi-Agency Coordination System housed at the State Emergency Operations Center. Agencies are directed to muster

their resources and work under a unified structure to maximize the efforts and ensure a coordinated response to mitigate the impacts and to return state government to a normal state as soon as possible. It is important that the local governments become educated about cybersecurity prior to an event and build this into to their emergency planning. Local governments must know in advance who to contact and the various means for making that contact when they suspect a potential cybersecurity event. It is important to anticipate that in a significant cyber event, such as a cyber disruption, normal channels of communications may be compromised or completely unavailable. Other Agencies should coordinate and align their cybersecurity strategies to this document.

Higher Education - Higher Education has been given responsibility for educating the next generation of cyber professionals. Commensurate with that responsibility, higher education is duty bound to engage their communities with expertise, outreach, and problem-solving to make Vermont more resilient. Higher Education must continue to develop its capabilities and programs to evolve with the threat and technology horizons, providing the talent to meet cybersecurity challenges. Higher education must engage with K-12 education developing interest in the field and building awareness in the students and faculty.

Business Community - The business community, which collects increasing amounts of citizen data such as credit card information, social security numbers, or biometric information, must take reasonable measures to safeguard the information in its control, be mindful of the information it is collecting, and comply with all laws regarding data security and data breach notification.

Vermont Citizens - The public at large has a responsibility to enact basic safety measures to protect themselves, to educate their children and monitor the activities of vulnerable relatives, including senior citizens, and to stay abreast of active scams and threats.

V. Next Steps

To successfully accomplish these cybersecurity strategy principles there are several steps the Cybersecurity Advisory Team must take. First, the CAT needs to understand the current security state of the various entities in Vermont. This review could include review of technological assets, configurations, polices, security controls, prior audits, vulnerabilities and other auditable aspects of cybersecurity. The goal is to understand where gaps exist, then to prioritize and close those gaps. The emphasis must be on predictive analysis in order to stop, limit, and mitigate future cyber-attacks.

The gaps identified during the review will then be part of an assessment to determine which gaps pose a high risk to their organization or to the state. Next, the CAT will develop objectives to mitigate the risk and close the identified gaps.

Many of the listed activities will be included in operational plans to be executed by some or all the groups listed under Roles and Responsibilities.

Some of the projects and initiatives created may deliver near-term outcomes. Other initiatives may have durations of many years and or may operate continually. The CAT will maintain responsibility to ensure that progress is tracked through meaningful metrics and reporting.

A lack of sufficient funding is the number one challenge states face, according to a study by NASCIO and Deloitte. Vermont is no different. The Governor, Legislators, State IT Leaders, Education, and Businesses must become strong advocates for funding cybersecurity. As we rely more on technology, we must unite in the commitment to effectively and proactively manage our cyber risks.

Historically Vermont's security budget has not been adequately funded to keep pace with technological advancements or the growing sophistication of threats. We recommend a subcommittee made up of Government and Private Industry experts to establish different methods of funding, based on the goals put forward in this strategy document. We expect a

blend of federal, state, and local funds, combined with private investment, to support future cybersecurity initiatives across the state.

VI. Conclusion

From Executive Order to strategy development, the Cybersecurity Advisory Team (CAT) has executed the charge given; to identify the strategic principles of cyber capability, cyber resilience, cyber communication, and cyber education as the core for building a strategy to protect data, information systems, and privacy of State government, Vermont businesses, and the public. Through describing the principles that guide strategy and operations; assigning roles and responsibilities for execution of this strategy; and identifying future actions, the CAT anticipates plans will be developed and actions taken toward the accomplishment of this strategy. Successful execution of this strategy will make significant strides towards building a Vermont that continues to be a safe and secure place to live, work and play.