

State Cybersecurity Principals & Best Practices

Cybersecurity is vital to both state government and industry. Improving and strengthening state government cybersecurity posture and resiliency is rightly a top priority. State governments have increasingly come to terms with the need for increased cybersecurity awareness and the need to secure state infrastructure for economic growth, prosperity, efficiency, and protection. All companies want a secure digital infrastructure to ensure successful growth of the IT industry and to harness future innovation. Companies design and build security into the DNA of their products and services and as a result they can provide a high level of cybersecurity to state governments. In the current environment of shrinking state budgets and ever-increasing cyber threats, the IT industry and states must partner together to protect state government digital assets.

The IT Alliance for Public Sector (ITAPS)¹ State Cybersecurity Acquisition Committee has established best practices for cybersecurity by examining ongoing state and federal initiatives that have proven to be both mature and effective in promoting a secure cyber environment. It is evident that state governments in general have struggled to adequately keep up with advances in cyber threats. To address this difficulty, ITAPS has created a broad set of cybersecurity principles for state governments to employ to better protect themselves from the increasing cyber threat.

To be most effective in enhancing cybersecurity, state and local governments can:


- **Partner with Industry.** State governments can leverage partnerships with the private sector by utilizing industry expertise through the acquisition of products and services with high levels of security and reasonable terms and conditions.
- **Adopt Industry-Recognized Security Standards.** State governments should adopt international standards recognized by industry to better align security across all agencies and departments.
- **Standardize Cloud Security.** If state governments plan on standardizing their approach to cloud security, they should leverage existing federal certification programs at the state level.
- **Establish an Outcome Focused Governance Structure.** A state's governance structure should cover all aspects of the enterprise and encourage cross-organizational collaboration and transparency.
- **Actively Share Information.** There are a wide variety of different models for the sharing of cyber threat information, and integration centers have emerged in recent years to provide a vital link between all levels of government, the private sector, and academia.
- **Create a Culture of Awareness.** State governments should invest in training and education for their workforces to enhance overall cybersecurity awareness.

Partner with Industry

The private sector owns and operates 85 percent of critical infrastructure in the United States, and the information technology industry supplies nearly the entire cyberspace infrastructure. As a result, the IT industry is the natural leader in the creation and deployment of cybersecurity tools, products, and services. States should look to the private sector to better defend their networks and data.

Many state agencies currently rely on a static approach to cybersecurity that often neglects proper cybersecurity hygiene. The IT industry is continuously monitoring, updating, and improving its cybersecurity in the rapidly evolving threat environment. IT vendors continue to improve their products and services in new

¹ **The IT Alliance for Public Sector (ITAPS)**, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies offering the latest innovations and solutions to public sector markets. With a focus on the federal, state and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants



and sophisticated ways to meet this need. To improve acquisition, state governments should rationalize and streamline security requirements that are unnecessarily burdensome, such as extensive paperwork and inordinately lengthy testing requirements. This will allow for faster acquisition and adoption of the latest, most secure solutions. States can also take advantage of the General Services Administration schedule 70 that include many of cyber products and solutions to protect state government networks and data.

State governments should also focus on developing terms and conditions that address cybersecurity and instances of data breach. Unlimited liability has been, and continues to be, a major concern for the IT sector. ITAPS has continuously advocated against high limitations of vendor liability, or in some cases uncapped liability, because it creates an unreasonably high risk for vendors and leads to higher costs for products and services for the state purchasing agency. These increased cost are subsequently passed off onto the taxpayers. ITAPS proposes that a rational limitation on damages be no more than the amounts paid by the state for the product or service that is the subject of the claim.

Many states have adopted these changes or already have reasonable limitations of liability but do not apply them in instances of data loss or data breach. States should ensure that they do in fact apply reasonable limitations on liability in the case of data breach to ensure the highest levels of competition during the RFP process. Vendors are generally unwilling and unable to underwrite extraordinary risk in states that have not adopted these changes.

Adopt Industry-Recognized Security Standards

It is important that states prioritize critical systems and data to ensure security of the state's most sensitive data. This prioritization will help achieve an effective, risk-based approach to protecting state systems. The state governments that are currently leading in cybersecurity have adopted and implemented security controls based on nationally recognized frameworks. Two of the leading and most commonly adopted frameworks are the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the International Organization for Standardization 27001 and 27002. Such frameworks can greatly improve a state's ability to protect its infrastructure and digital assets.

Existing international frameworks can help states leverage proven standards without having to create costly and less known security practices. Adoption of existing frameworks will help assess program effectiveness and identify and address weaknesses in state systems. It is critical that states take a multi-faceted approach to cybersecurity and follow these well-established standards that will ensure consistency across all levels of government. States should allow for the use of technologies that align with international, market-driven standards. This enables technology companies to focus their resources on enhancing security solutions that can scale for the national and global market, rather than making a multitude of adjustments to ensure compliance with a series of static requirements and specifications.

Although only issued in February 2013, the most frequently adopted standard across state governments is the NIST Cybersecurity Framework. The NIST Cybersecurity Framework was developed over the course of 10 months by highly qualified cybersecurity professionals both within the federal government and industry, including significant input provided by the Information Technology Industry Council.

The NIST framework provides an assessment mechanism that allows state governments to determine their current cybersecurity capabilities, set individual goals, and establish a plan for improving and maintaining cybersecurity programs. The Framework is not a prescriptive approach to cybersecurity and is not a one-size fit all process. The framework is a risk-based compilation of guidelines designed to help organizations assess current capabilities and draft a prioritized roadmap toward improved cybersecurity practices. Many state



governments have committed to adopting the NIST Framework and to mapping their own security protocols against the NIST Framework.

The NIST Cybersecurity Framework encourages states to immediately conduct an independent operational risk assessment of state infrastructure, applications, and data to determine the highest risk across the government and subsequently prioritize and appropriately resource remediation with specific completion dates. Additionally, the NIST Cybersecurity Framework helps facilitate the development and execution of strategies to keep systems on the most up-to-date security versions enabling a state to mitigate the risk posed by systems that cannot be immediately updated. ITAPS recommends states leverage the NIST Cybersecurity Framework to protect state systems.

Standardize Cloud Security

As more state governments leverage the full capabilities and potential of cloud services, their cybersecurity models will be radically transformed. Cloud computing has become mainstream as governments at all levels have realized its benefits. Cloud services enable states to achieve operational efficiencies, instant scalability, price elasticity, expanded computational and processing power, and provide cost reductions. Adoption of cloud computing can also help state governments improve information security.


States should leverage existing federal efforts such as the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud computing products and services. FedRAMP can provide states insight into approved cloud security services and can save states time and money by not having to develop their own individual security assessment products. Many cloud computing providers are already compliant with FedRAMP standards, while many more are in the process of becoming compliant. Preference should be provided to those that have obtained FedRAMP approval, and states should utilize FedRAMP certification to better inform their acquisition of quality cloud products and services.

Establish an Outcome Focused Governance Structure

States must begin to escalate security from merely an IT concern to a business risk concern. This can be done by allowing the state Chief Information Security Officer (CISO) to make critical security decisions. A state CISO should have the authority to create minimum information security requirements for each agency to follow including more stringent standards for agencies with sensitive information. Additionally, each agency should develop, document, and implement its own information security plan, which must be approved by the state CISO. The information security plan should be made available for public comment. The CISO should work with each agency to create security awareness training to inform personnel, including contractors, who operate any agency information system. The CISO should periodically perform full-scale testing and evaluation of the effectiveness of information security systems, procedures, and practices. Lastly, each year an agency should perform an independent evaluation of their security program and procedures. This evaluation should be conducted by an independent external auditor to eliminate bias and increase effectiveness.

Actively Share Information

Other steps that state governments have taken, albeit at varying degrees of engagement, include participating in a number of information security sharing organizations. For instance, the Multi-State Information Sharing and Analysis Center provides continuous real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and support in mitigation and incident response. States can also leverage Fusion Centers, which operate as focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, state, local, and private sector partners. The National Governors Association's Resource Center for State Cybersecurity also provides a collaborative effort for not only governors but also CIOs, CISOs, and state homeland security advisors. There are a wide variety of different



models for the sharing of cyber information and integration centers have emerged in recent years to provide a vital link between governments, the private sector, and academia.

Create a Culture of Awareness

It is critical that state governments understand the risks cyber threats pose to property, reputations, and operations. Many state agencies and departments are not aware or fail to use the range of cybersecurity tools available to them, such as information sharing, risk management models, training, nationally accepted security standards, guidelines, and best practices. Raising awareness so that state governments can use these tools is critical to improving cybersecurity.

Information security should be a core part of the state's organizational culture. While the predominant method to combat cyber risks is to pursue the latest security products, tools, and technology plans, that effort alone is insufficient to a holistic cybersecurity approach. State governments must increase their focus educating and training employees, which requires them to provide adequate funding for such efforts. Information security training should be mandatory for all government employees and contractors, and information security performance should be an item in performance reviews. State governments should optimize enterprise and workforce planning to leverage consolidation in security talent, achieving cost savings and security benefits. This involves certain functions that are not inherently governmental to be outsourced, such as data centers shifting to vendor managed cloud environments with pre-defined security parameters. Lastly, it's important that state officials and state legislators view cybersecurity as a continuous and ongoing process. Cybersecurity that is subject to inconsistency in funding and lack of attention will create enormous vulnerabilities that will be exploited if they are not addressed in a consistent manner.

Conclusion

While cybersecurity represents a significant challenge at all levels of government, the IT industry is adapting and creating a multitude of opportunities to provide new services and products that can be used to provide high levels of protection for states and their citizens. State, national, and global governments must work with the private sector, academia, and public stakeholders to develop and implement cybersecurity policies that improve security, enable innovation, and build public trust. Industry is eager and willing to share its expertise to better protect state infrastructure and will continue to embrace partnerships with state and local governments.